

Handbuch / KENDOX WebService

Stand:29. September 2014

1 Inhaltsverzeichnis

2 Änderungen

Dieses Kapitel soll einen Überblick über die Neuerungen dieses Handbuchs verschaffen.

Kapitel	Version	Änderung
	4.0	Neues Handbuch erstellen
7.3, 8.2, 10.1, 10.3, 10.4, 11.4, 13.3, 16.3	4.0.16	In der "ConnectionPoolSettings.xml"-Datei wurden wurden die Einträge <FileExportDirectory>, <FileImportDirectory>, <AnnotationTemplatesDirectory>, <DockingLayoutTemplateDirectory>, und <DockingLayoutDirectory> durch den Eintrag <TempDirectory> ersetzt. Somit wird die Rechtevergabe der temporären benötigten Verzeichnisse vereinfacht.
11.4	4.0.20	Verzeichnisberechtigungen aktualisiert.
9.2, 10.2	4.0.29	Der Application Pool muss als "ASP.NET 4.0 Integrated" konfiguriert sein.
12, 12.1	4.0.52	Zwei-Faktor-Authentifizierung dokumentiert
9.4	4.0.57	WebService Autostartfunktion im IIS
9.4	4.0.57	Beispielsetup unter IIS 8 durchgeführt

3 Allgemein

3.1 Was ist Kendox WebService?

Kendox WebService ist eine Anwendung, welche die Kommunikation zwischen mehreren Kendox Produkten gewährleistet. Kendox WebService bildet somit einen Knotenpunkt im Netz der Anbindung ans Web. Darüber hinaus dient Kendox WebService als Schnittstelle für externe Programme für den Zugriff auf den InfoShare.Server.

3.2 Wo kann Kendox WebService in der Praxis angewandt werden?

Kendox WebService kommt überall dort zum Einsatz, wo Daten plattformunabhängig vom InfoShare-Server abgerufen werden sollen (z. B. von einer Java-Anwendung). Der Kendox WebService steht immer in Verbindung mit einer Anwendung, die auf den InfoShare-Server zugreifen soll. Solche Anwendungen sind z. B. Kendox RIA.Client oder KendoxWeb.

3.3 Kompatibilität zu Kendox ConverterService

Die Funktionalität der vorigen ConverterService-Versionen 1.1.x bleibt in den neuen Versionen 2.0.x erhalten (Abwärtskompatibilität). Das heisst, dass alle Kendox WebService-Versionen den neuen ConverterService 2.0.x verwenden können.

3.4 ConverterService – Bestandteil von Kendox WebService

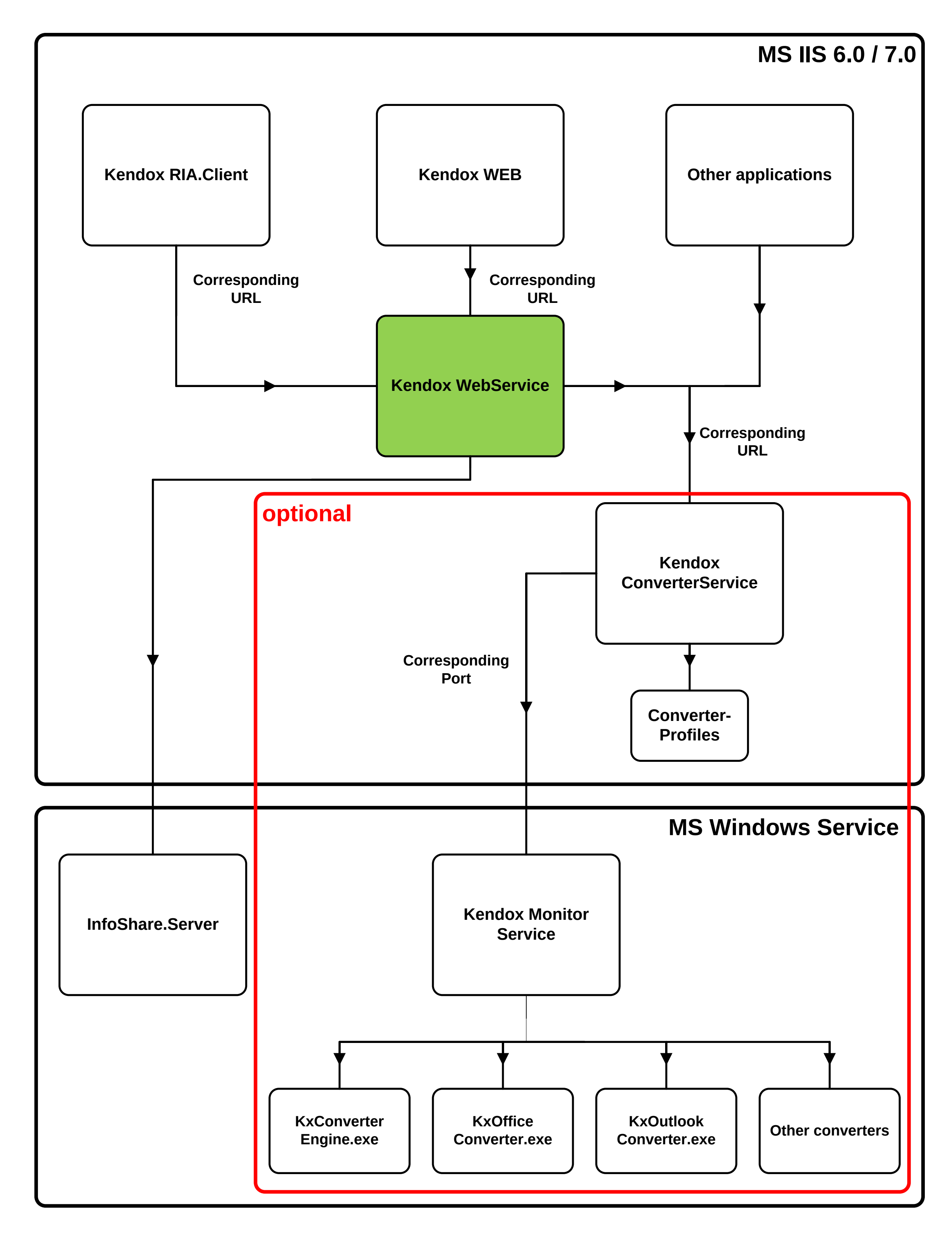
Der Kendox ConverterService ist in den Kendox WebService 4.0 integriert. Soll der integrierte ConverterService genutzt werden, darf in der ConnectionPoolSettings.xml-Datei keine ConverterService-URL im <ConverterWebServiceUrl>-Tag hinterlegt werden.

Der integrierte ConverterService bietet eine bessere Performance bei grösseren Dokumenten, da die Dokumentdaten nicht über das SOAP-Protokoll zwischen den WebServices übertragen werden müssen.

Die Konfiguration/Definition der einzelnen Konvertierungsprofile ist aus dem Handbuch Kendox ConverterService zu entnehmen. Die Konfigurationsdatei Profiles.xml, in der die Konvertierungsprofile angelegt werden, befindet sich im Hauptverzeichnis des Kendox WebServices.

4 Funktionsschema

Das folgende Schema zeigt die Einbettung und auch die Funktionsweise von Kendox WebService. Einerseits sind die Produkte aufgeführt, welche von Kendox WebService verwendet werden, andererseits auch diejenigen, welche Kendox WebService für ein reibungslose Ausführung benötigt.



5 Lizenzierung und Lizenzverzeichnis

In Kendox WebService werden die Lizenzdateien (auch von Kendox RIA.Client) zentral verwaltet. Dazu existiert im Installationsverzeichnis von Kendox WebService (standardmässig unter dem Pfad „C:\Inetpub\wwwroot\KXWebService\“) das Verzeichnis „Licenses“. Für jede Applikation existiert ein eigenes Unterverzeichnis im Verzeichnis „Licenses“, in dem die Lizenzdateien (*.bck) der einzelnen Applikationen abgelegt werden. Für nähere Informationen zur Lizenzierung von Kendox RIA.Client steht ein eigenständiges Handbuch „Kendox RIA.Client“ zur Verfügung.



Hinweis: Für Kendox WebService wird zurzeit keine Lizenzdatei benötigt. Kendox WebService überprüft die Lizenzdateien von Kendox RIA.Client.

Wichtig ist, dass auf das Verzeichnis „Licenses“ und auf die darunter liegenden Verzeichnisse und Dateien **Lesezugriff** für die folgenden Benutzer gesetzt sind:

- Benutzer, unter dem der Kendox WebService läuft, wenn die Formular-authentifizierung aktiviert ist (kein Single-Sign-On).
- Alle Single-Sign-On-Benutzer (falls Single-Sign-On aktiviert ist).



Achtung: Bitte auf die Gross- und Kleinschreibung des Hostnamens bei der Bestellung der Lizenzdatei achten! Ansonsten funktioniert die Lizenzdatei nicht.

---

6 Installationsübersicht WebService / Kendox RIA.Client

1. Installation / Konfiguration IIS 6/7
    a. IIS 6-Kompatibilitäts-Features installieren
    b. WWW-Dienste installieren
    c. Berechtigung auf temporären Ordner (z. B. „KXWebServiceTemp“) für Benutzer IUSR und IIS_WPG (und alle Single-Sign-On-Benutzer*)
2. Installation Microsoft .NET Framework 4.0
    a. Prüfen, ob ASP.NET 4.0 unter „ISAPI and CGI Restrictions“ als „Allowed“ aufgeführt sind
3. Ausführen der Kendox WebService MSI-Datei
4. Konfiguration WebService
5. Konfigurationsdatei „ConnectionPoolSettings.xml“ bearbeiten
6. Konfigurationsdatei „URLEncryptionSettings.xml“ bearbeiten
7. *Single-Sign-On (ADS-Integration) konfigurieren
8. **Lizenzdatei für RIA.Client in entsprechenden „Licenses“-Ordner kopieren
9. **Konfiguration RIA.Client

*nicht zwingend erforderlich
** nicht erforderlich, wenn kein Kendox RIA.Client im Einsatz ist

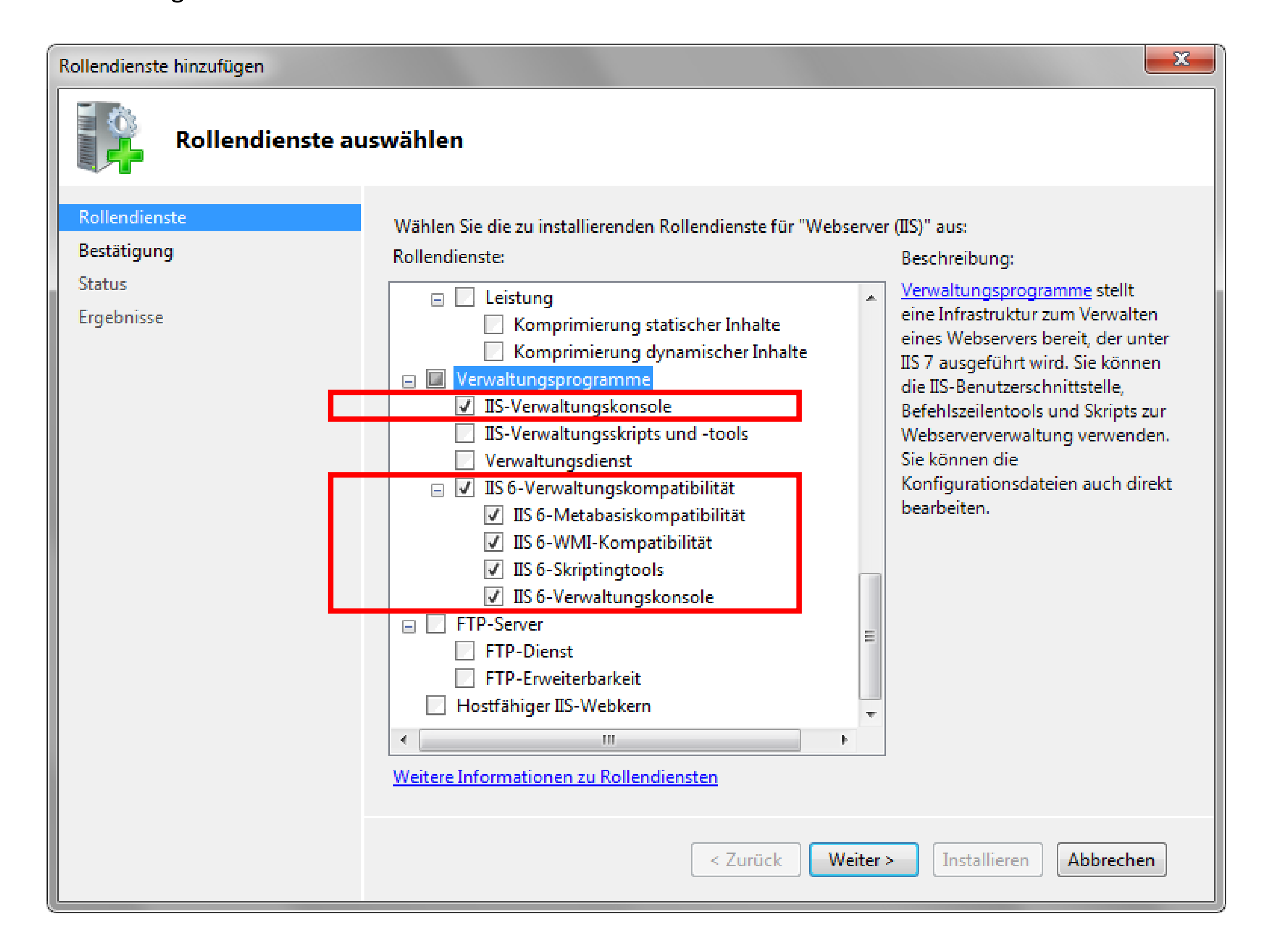
7 Konfiguration IIS 7

Bei der Installation von Kendox WebService und RIA.Client auf einem Windows Server 2008, Windows 7 oder Windows Vista müssen die folgenden Punkte beachtet werden, da ansonsten die beiden genannten Kendox-Produkte nicht funktionieren:

7.1 Windows Server 2008 R2

IIS 6-Kompatibilitäts-Features installieren

Im Startmenü muss „Verwaltung“ → „Server-Manager“ geöffnet werden. Im Bereich „Rollen“ → „Webserver (IIS)“ ist „Rollendienste hinzufügen“ auszuwählen. Im darauf öffnenden Fenster müssen folgende Funktionen aktiviert werden:



WWW-Dienste installieren

Im Startmenü unter „Verwaltung“ → „Server-Manager“ → „Rollen“ → Bereich „Webserver (IIS)“ müssen die folgend aufgelisteten „WWW-Dienste“ installiert sein.

Allgemeine HTTP-Features

- Statischer Inhalt
- Standarddokument
- Verzeichnissuche
- HTTP-Fehler

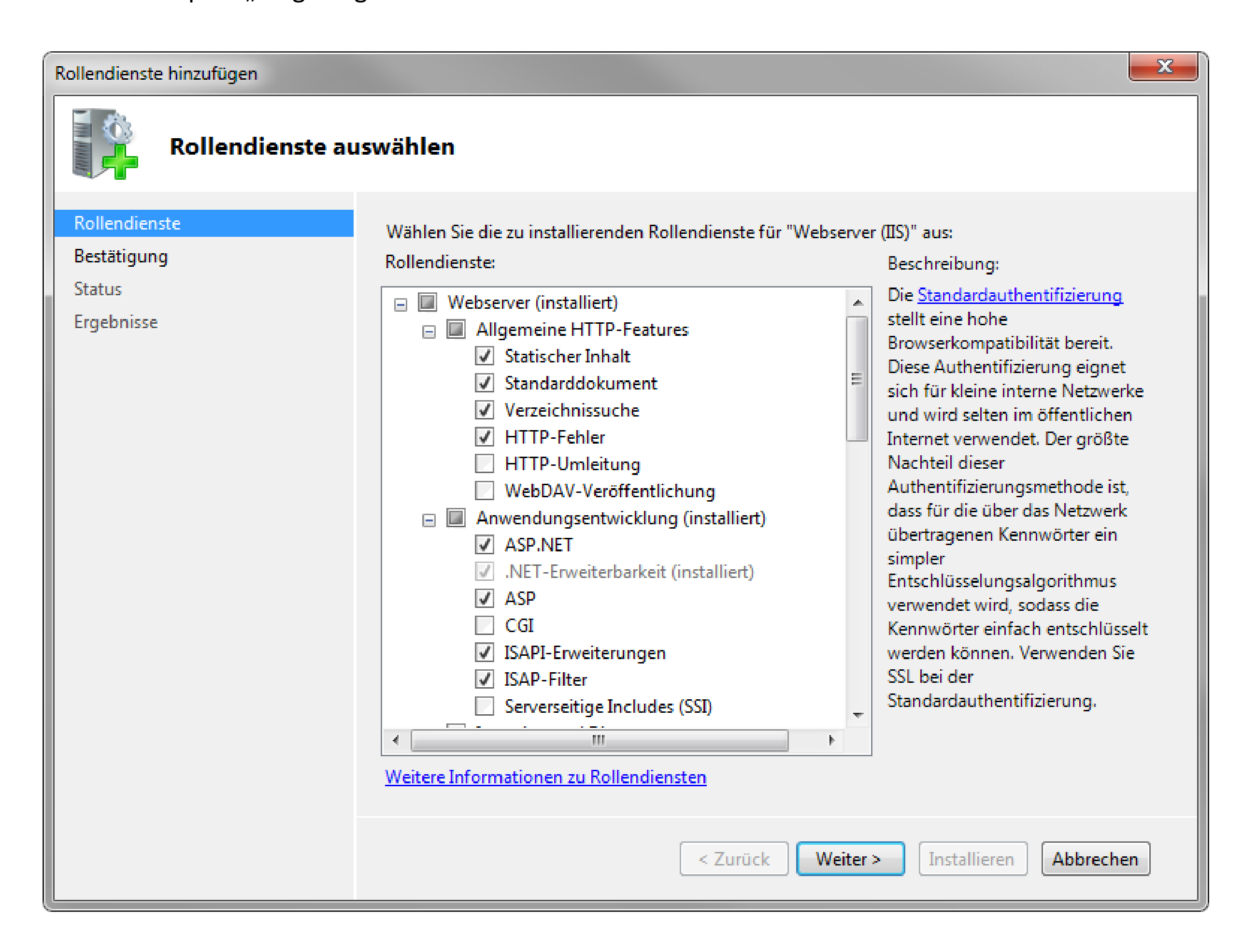
Anwendungsentwicklung

- ASP.NET
- .NET-Erweiterbarkeit (installiert)
- ASP
- ISAPI-Erweiterungen
- ISAP-Filter

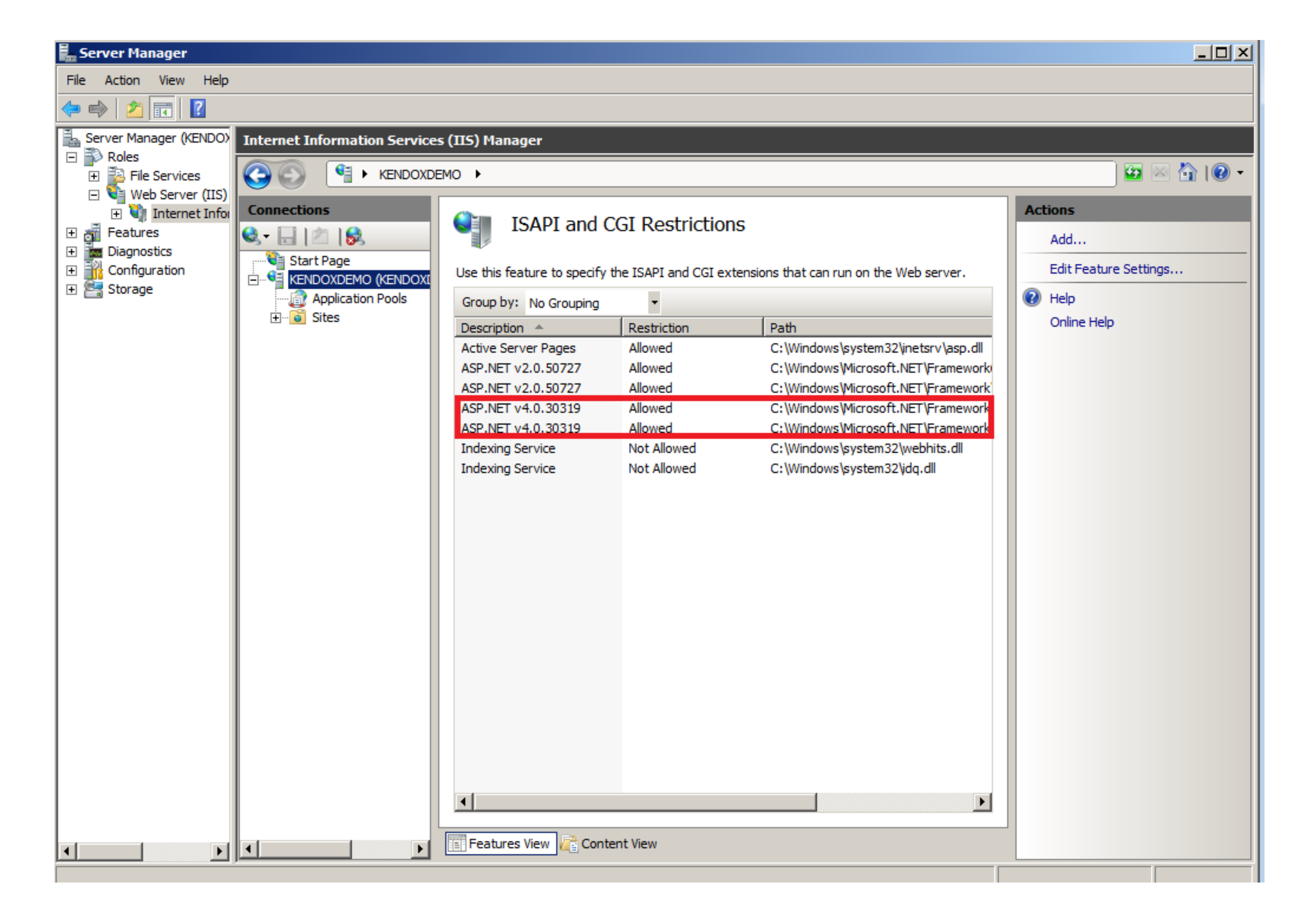
Sicherheit (nur für Single-Sign-On)

- Standardauthentifizierung
- *Windows-Authentifizierung
- Anforderungsfilterung

* Diese Features sind nur dann erforderlich, wenn SSO verwendet wird. Für die Konfiguration für SSO siehe Kapitel „Single-Sign-On“.



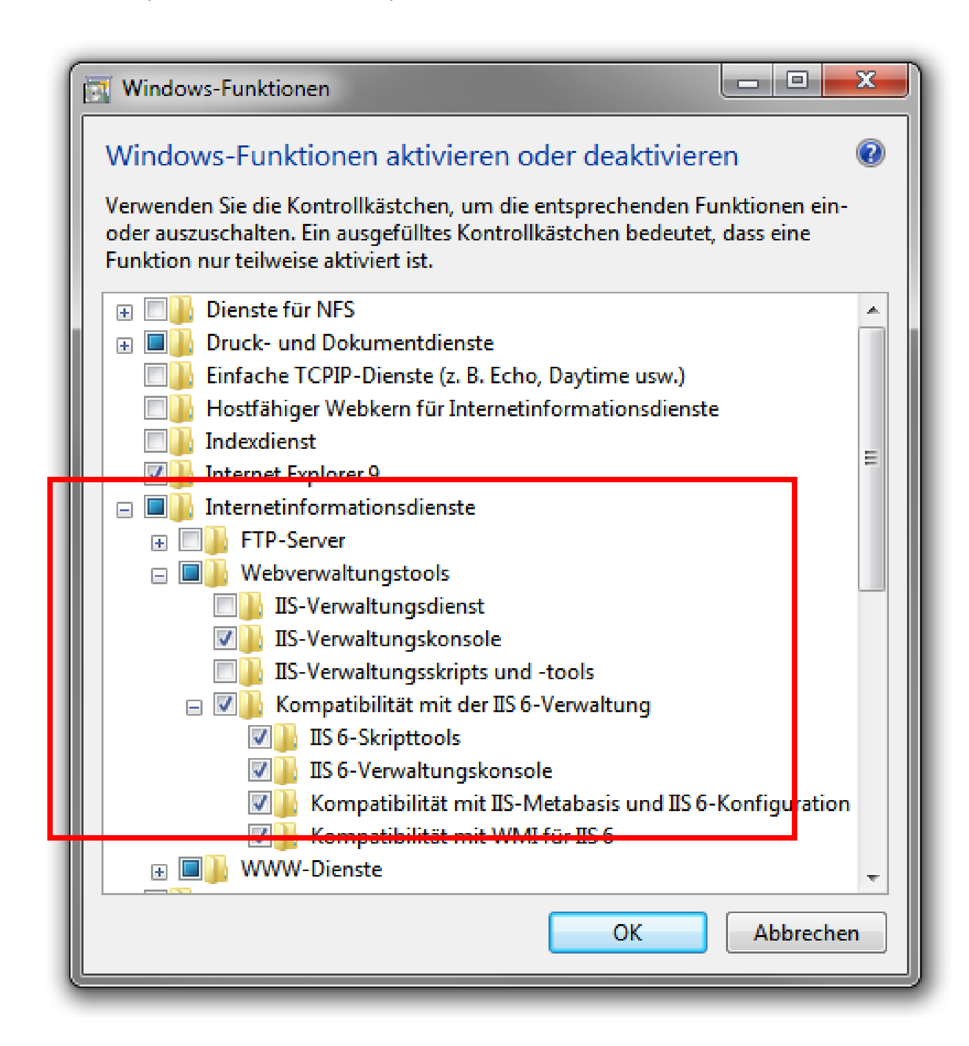
Nach erfolgreicher Installation des IIS und Microsoft .NET Framework 4.0 muss geprüft werden, ob in der „ISAPI and CGI Restrictions“ die ASP.NET 4.0 Erweiterung als „Allowed“ gekennzeichnet ist. Falls nicht, muss diese auf „Allowed“ gesetzt werden.



7.2 Windows Vista / 7

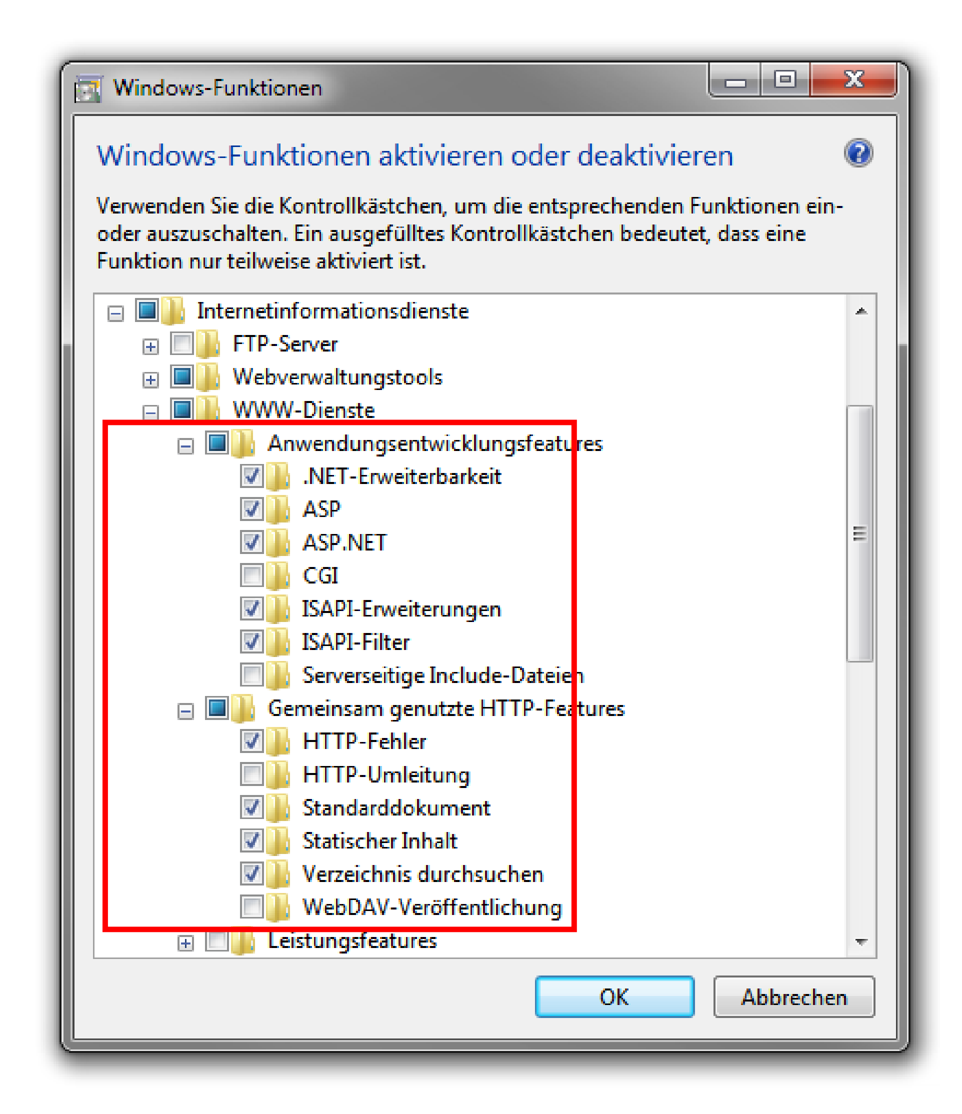
IIS 6-Kompatibilitäts-Features installieren

Unter „Systemsteuerung“ → Kategorie „Programme“ → Kategorie „Programme und Funktionen“ → „Windows-Funktionen aktivieren oder deaktivieren“ müssen folgende Features installiert werden (siehe Bildausschnitt).



WWW-Dienste installieren

Unter „Systemsteuerung“ → Kategorie „Programme“ → Kategorie „Programme und Funktionen“ → „Windows-Funktionen aktivieren oder deaktivieren“ müssen die folgenden „WWW-Dienste“ installiert werden (siehe Bildausschnitt).



Wird ein 64-Bit-Betriebssystem verwendet, muss der IIS 6 im 32-Bit-Modus verwendet werden. Anleitungen, wie der Modus (32-Bit, 64-Bit) im IIS 6 umgestellt/konfiguriert wird, können unter den folgenden Links bezogen werden:

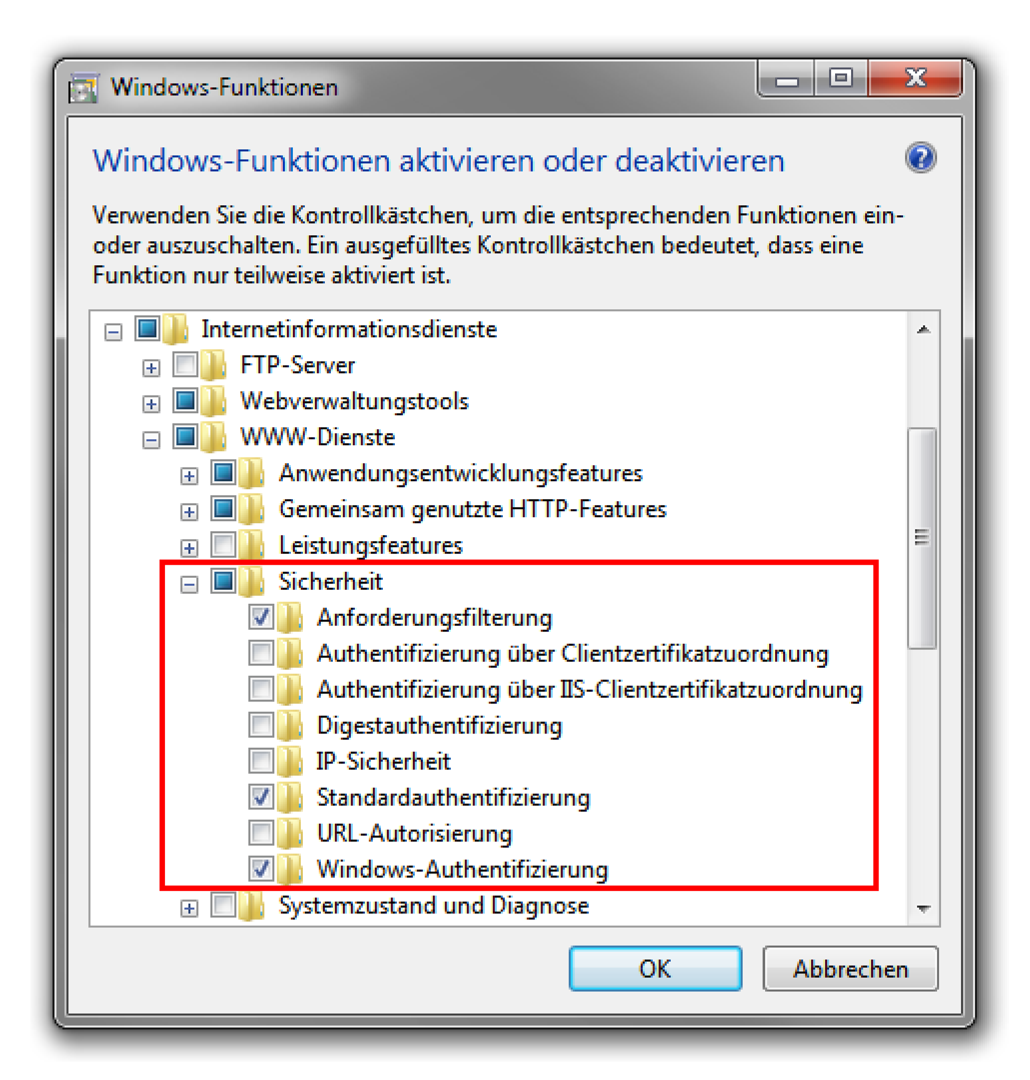
- http://support.microsoft.com/kb/894435
- http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0aafb9a0-1b1c-4a39-ac9a-994adc902485.mspx?mfr=true

Unter IIS 7 können Applikationen mit 32-Bit oder 64-Bit betrieben werden (Mischbetrieb). Je nach Wunsch oder Bedürfnis können einzelne Applikationen im 32bit- oder 64bit-Modus laufen:
- http://blogs.msdn.com/rakkimk/archive/2007/11/03/iis7-running-32-bit-and-64-bit-asp-net-versions-at-the-same-time-on-different-worker-processes.aspx

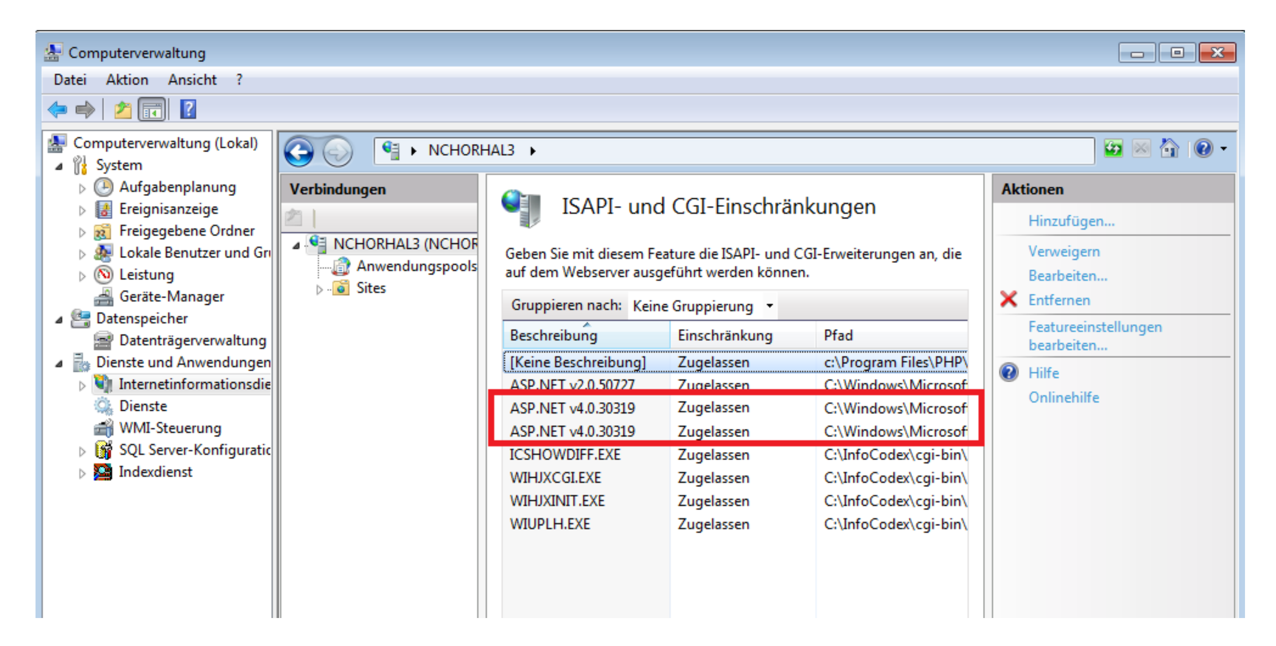
Single-Sign-On-Feature installieren

Soll „Single-Sign-On“ (kurz SSO) verwendet werden, müssen folgende Sicherheits-features im IIS 7 installiert werden:

Unter „Systemsteuerung“ → Kategorie „Programme“ → Kategorie „Programme und Funktionen“ → „Windows-Funktionen aktivieren oder deaktivieren“ müssen die folgenden Features unter „WWW-Dienste“ → „Sicherheit“ installiert werden (siehe Bildausschnitt).
Diese Features sind nur dann erforderlich, wenn SSO verwendet wird. Für die Konfiguration für SSO siehe Kapitel „Single-Sign-On“.



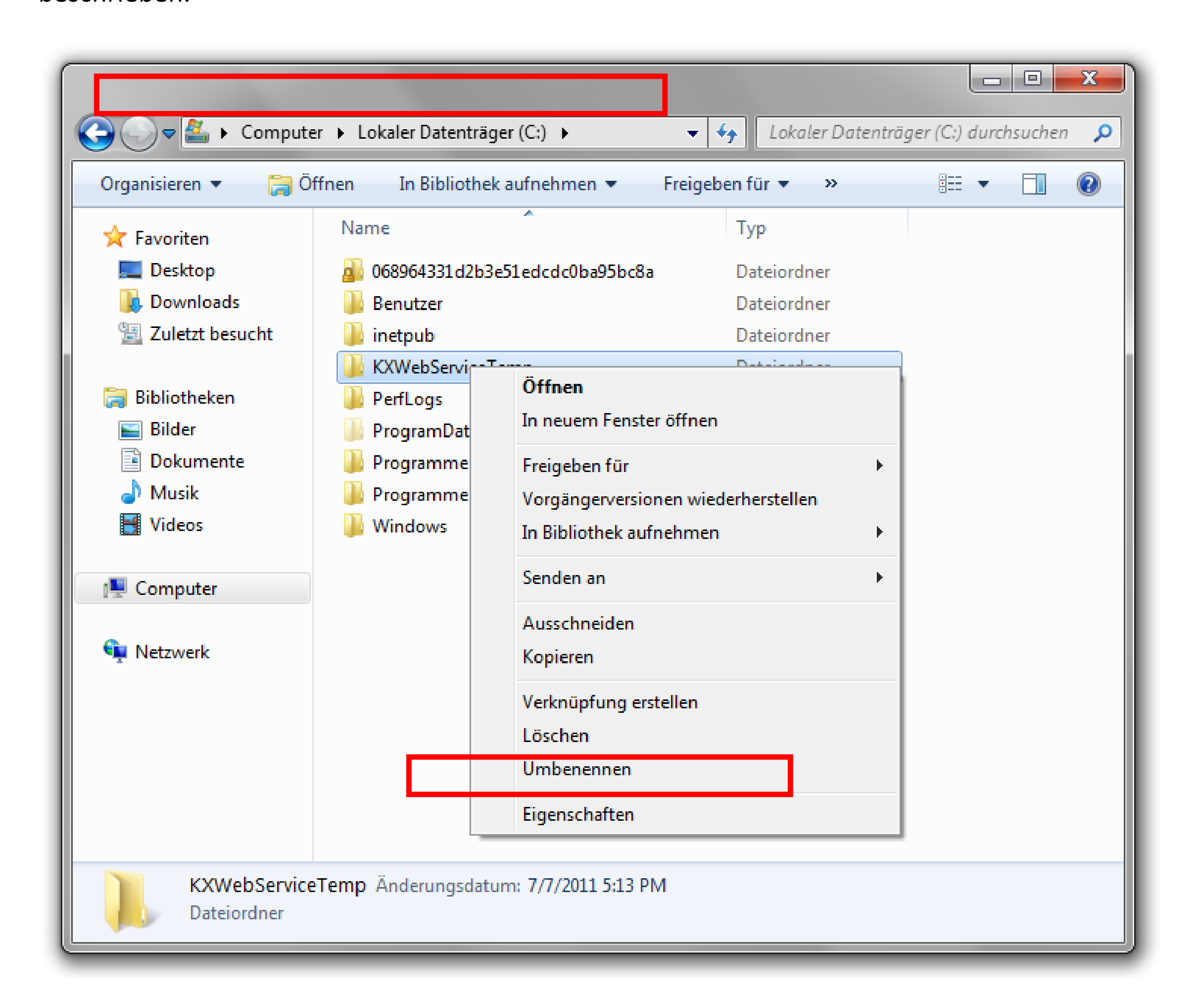
Nach erfolgreicher Installation des IIS und des Microsoft .NET Framework 4.0 muss geprüft werden, ob die ASP.NET 4.0 Erweiterung in den „ISAPI- und CGI-Einschränkungen" als „Zugelassen" gekennzeichnet sind. Falls nicht, müssen die Erweiterungen auf „Zugelassen" gesetzt werden.



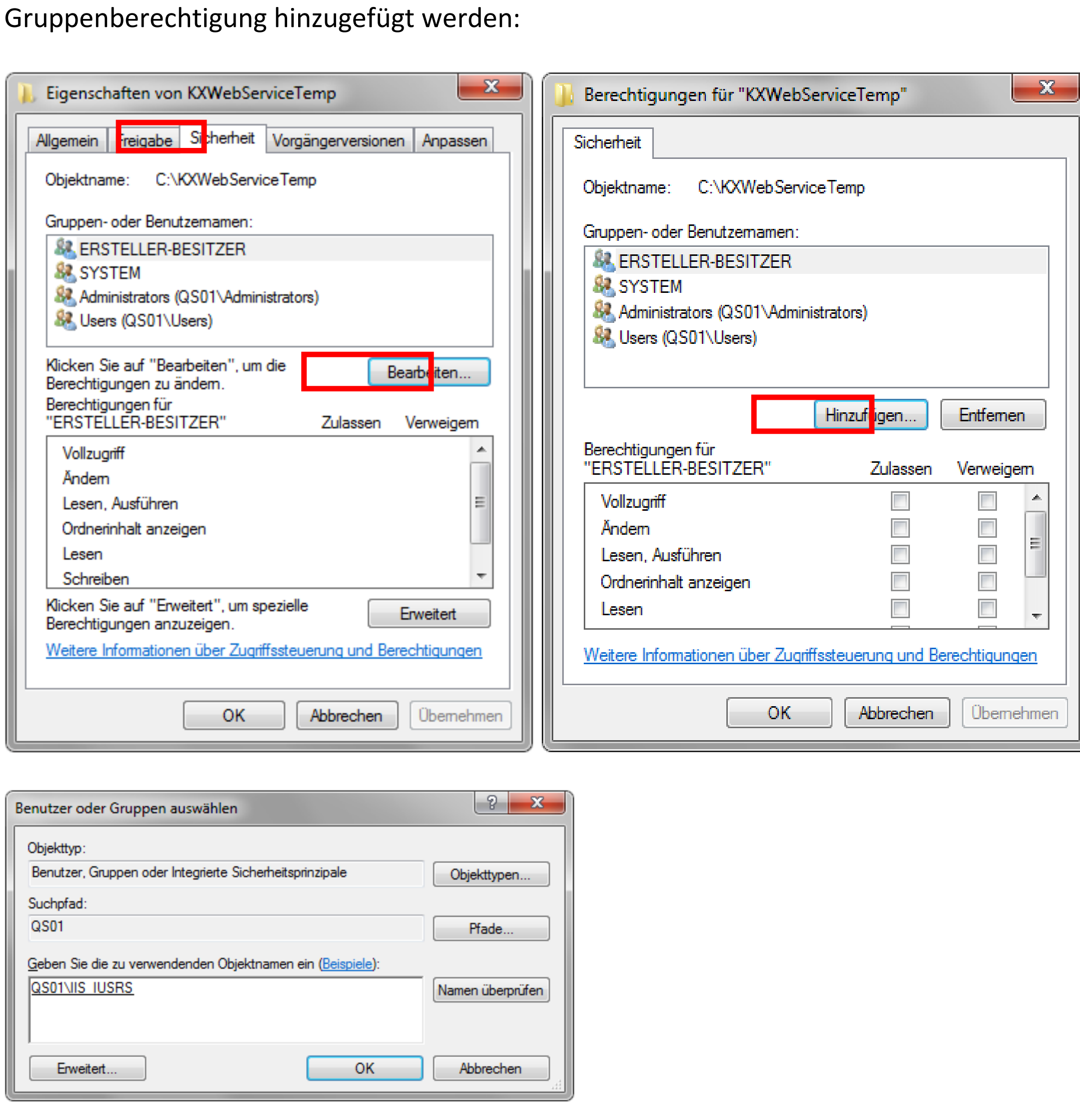
7.3 Benutzerberechtigungen IIS 7

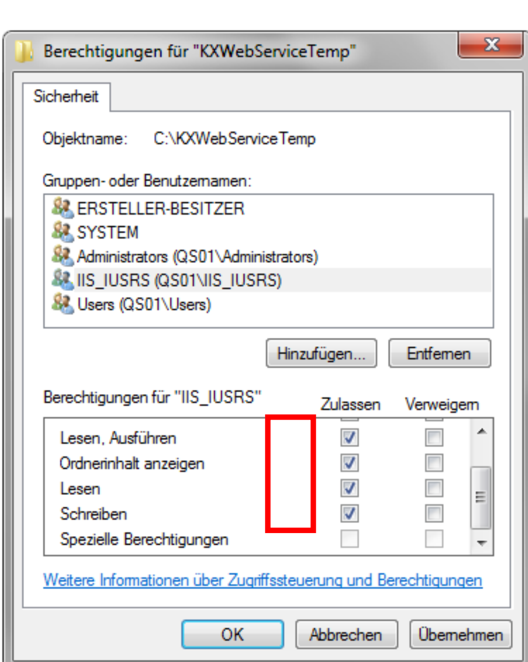
Bei IIS 7 muss die Benutzergruppe „IIS_IUSRS“ Schreib-, Lese- und Veränderungsrechte auf das Verzeichnis „KXWebServiceTemp“ besitzen. Im unten angeführten ScreenShot wird das temporäre Verzeichnis auf C:\KXWebServiceTemp gelegt. Wird in der Konfiguration KEIN explizites Verzeichnis definiert, wird das Verzeichnis relativ zum Root-Verzeichnis des Kendox WebService Installationsverzeichnisses gesucht (z.B. „C:\inetpub\wwwroot\KXWebService\KXWebServiceTemp“).

Bei Single-Sign-On müssen auch alle Single-Sign-On-Benutzer Zugriff auf das Verzeichnis „KXWebServiceTemp“ besitzen. Eine detaillierte Konfiguration ist im Kapitel „Single-SignOn“ beschrieben.



Es ist möglich, dass die Gruppe in der Liste nicht existiert. Unter „Bearbeiten“ kann die Gruppenberechtigung hinzugefügt werden:





8 Konfiguration IIS 6

8.1 32-Bit-Modus einschalten

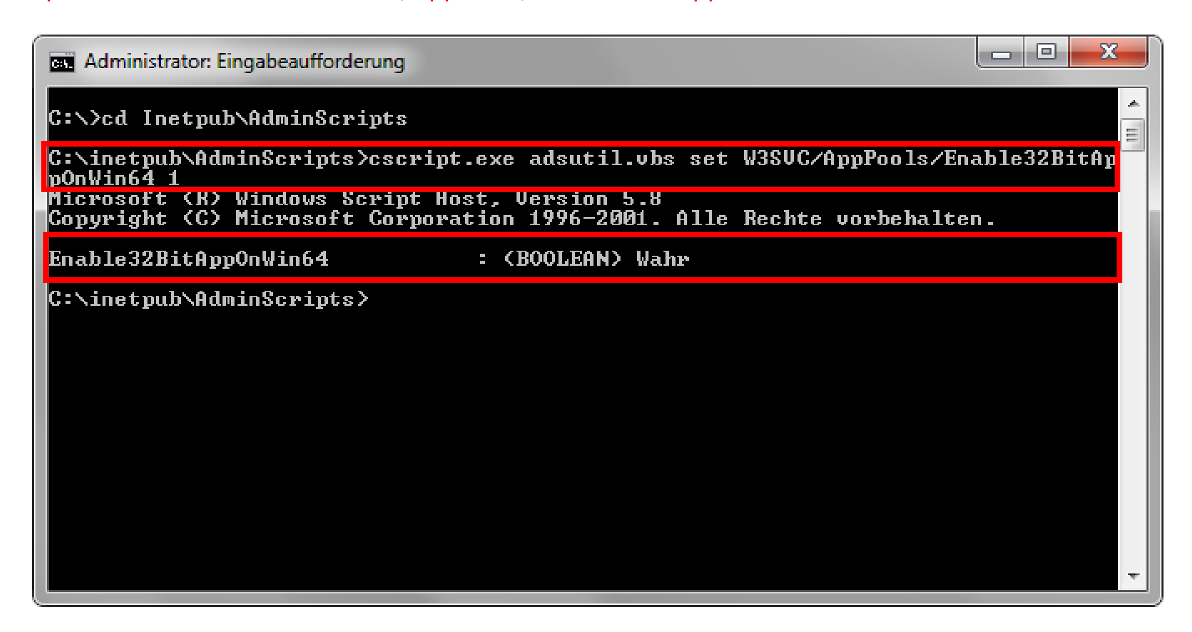
Bei der Verwendung eines 64-Bit-Betriebssystems muss der IIS 6 im 32-Bit-Modus verwendet werden. Für IIS 7 mit IIS 6 Kompatibilität gilt dies nicht.

Umschalten des IIS 6, um 32-bit Webapplikationen auf einem 64-Bit Windows zu betreiben:

1. In der Windows Konsole in das Verzeichnis ***%windir%\Inetpub\AdminScripts*** wechseln.

2. Folgenden Befehl ausführen:

cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 1



Quelle

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0aafb9a0-1b1c-4a39-ac9a-994adc902485.mspx?mfr=true

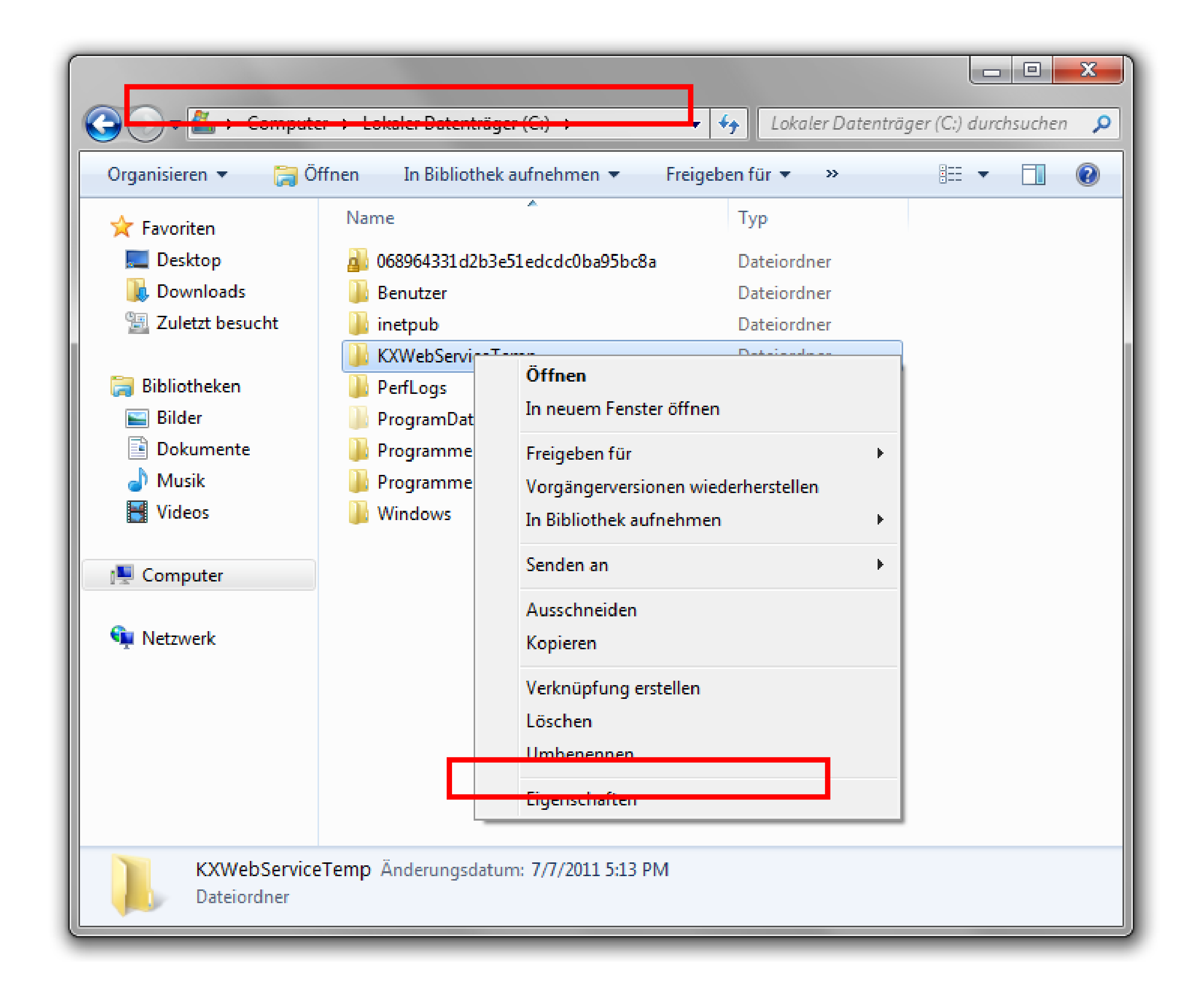
Der IIS 6 kann entweder im 32-Bit oder 64-Bit-Modus betrieben werden. Ein Mischbetrieb wie im IIS 7 ist nicht möglich.

8.2 Benutzerberechtigungen

Die Benutzer „IUSR_[Computername]“ und „IIS_WPG“ (oder „[Computername]\ ASPNET“) müssen Schreib-, Lese- und Veränderungsrechte auf das Verzeichnis „KXWebServiceTemp“ besitzen. Im unten angeführten ScreenShot wird das temporäre Verzeichnis auf C:\KXWebServiceTemp gelegt. Wird in der Konfiguration keine explizites Verzeichnis definiert, wird das Verzeichnis relativ zum Root-Verzeichnis des Kendox WebService Installationsverzeichnisses gesucht (z.B. „C:\inetpub\wwwroot\ KXWebService\KXWebServiceTemp“).

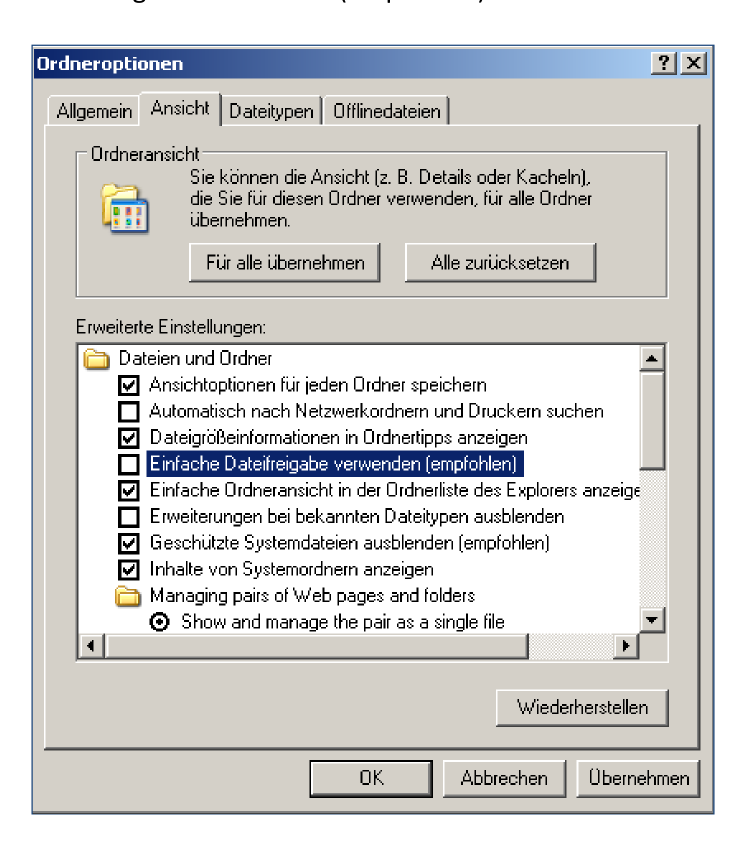
Als alternative Lösung kann der Benutzer „IUSR_[Computername]“ mit einem Benutzer ersetzt werden, der genügend Rechte für den Dateiexport hat.

Bei Single-Sign-On müssen alle Single-SignOn-Benutzer Zugriff auf das Verzeichnis „KXWebServiceTemp“ besitzen. Eine detaillierte Konfiguration ist im Kapitel „Single-SignOn“ beschrieben.



Falls der Computer nicht in einer Domäne ist, existiert der Reiter „Sicherheit“ unter Windows XP möglicherweise nicht. Um den Reiter „Sicherheit“ zu aktivieren, muss die folgende Option deaktiviert werden:

Im Windows-Explorer → „Extras“ → „Ordneroptionen“ → „Ansicht“ → Eintrag „Einfache Dateifreigabe verwenden (empfohlen)“ deaktivieren.



9 Kendox WebService Installation im IIS

9.1 ASP.Net-Benutzer für IIS registrieren

Wurde das Microsoft .NET Framework 4.0 vor dem IIS installiert oder wurden nachträglich IIS-Komponenten installiert, muss der ASP-Benutzer bei .NET neu registriert werden:

1. Mit „Start“ → „Ausführen…“ → Befehl „cmd“ die Windows-Konsole öffnen.

2. In der soeben geöffneten Konsole den folgenden Befehl eingeben:

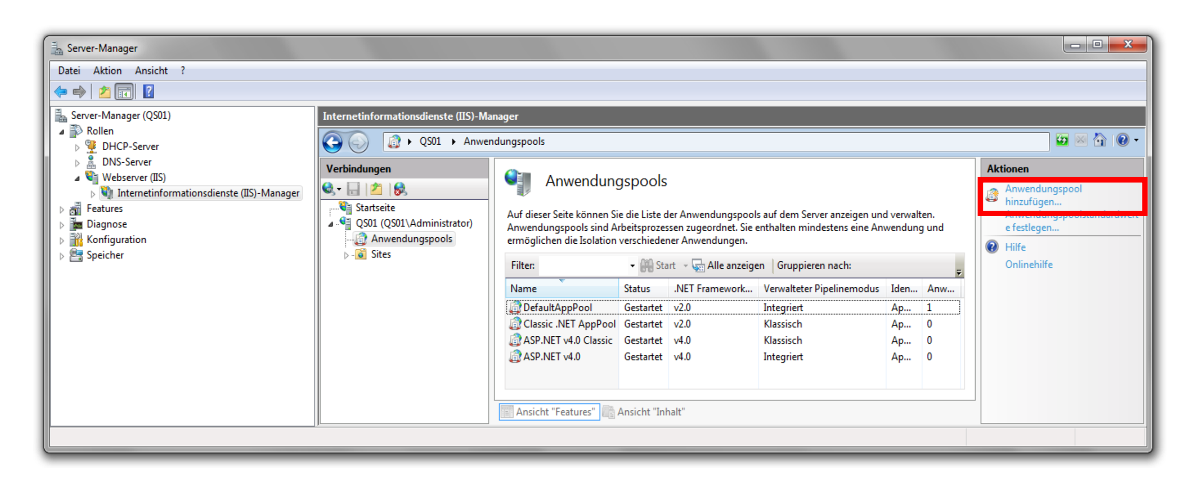
   cd C:\Windows\Microsoft.NET\Framework\v4.0.30319

   → Der Befehl „cd“ wechselt in den obigen Pfad.
   → Nun sollte folgender Pfad geöffnet sein:
   C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319
   → Achtung, Version (hier V4.0.30319) kann abweichen!

3. Folgende Befehle in der Command-Line nacheinander ausführen:
   aspnet_regiis.exe –i
   aspnet_regiis.exe –i -enable

9.2 Installieren von Kendox WebService

1. Im Server-Manager können unter „Rollen“ → „Webserver (IIS)“ → „Internetinformationsdienste (IIS)-Manager“ alle Anwendungspools angezeigt werden. Kendox empfiehlt, für Kendox WebService und RIA.Client je einen eigenen Anwendungspool zu erstellen (siehe rote Markierung). Es können aber auch bestehende Pools konfiguriert und verwendet werden. Für Kendox WebService und RIA.Client muss ein Application Pool „.NET Framework 4.0 integrated“ verwendet werden.



2. Starten der MSI-Installationsdatei für den Kendox WebService:

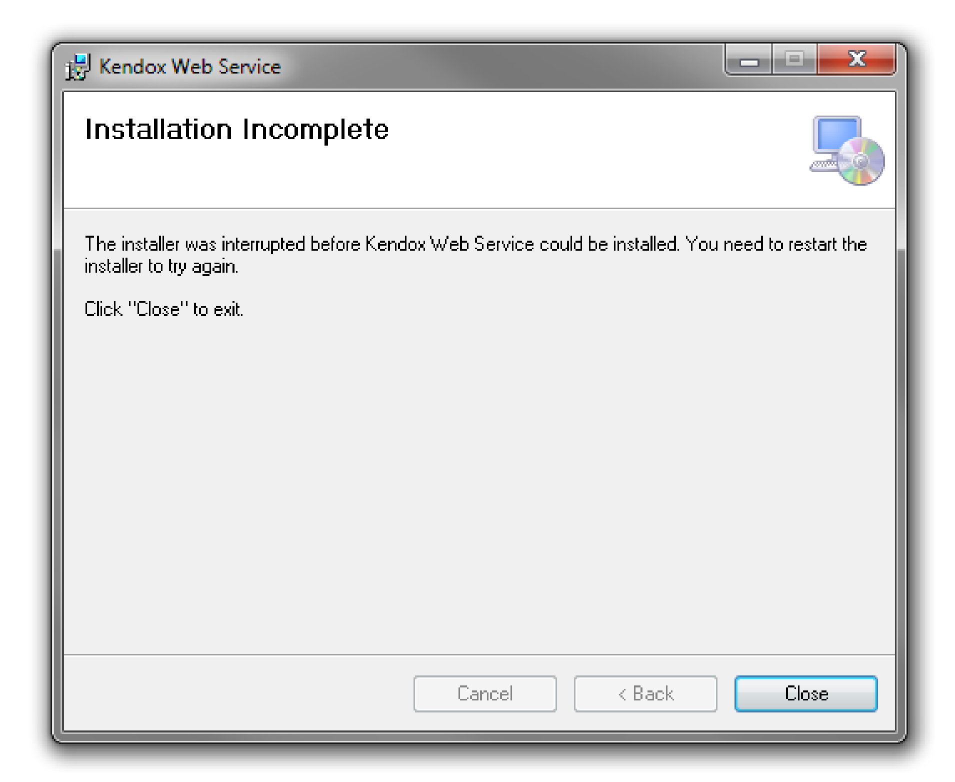
   Bei Windows Vista, Windows 7, Windows 8 oder Windows Server 2008 ist es zwingend, dass das MSI-Paket als Administrator ausgeführt wird („Als Administrator ausführen"). Ist dies nicht möglich, muss die Datei „MsiRunAsAdmin.reg" ausgeführt werden. Diese REG-Datei liegt in der ZIP-Datei von Kendox WebService.

   Hat der angemeldete Benutzer keine oder nur beschränkte Administrationsrechte, erscheint folgende Meldung:

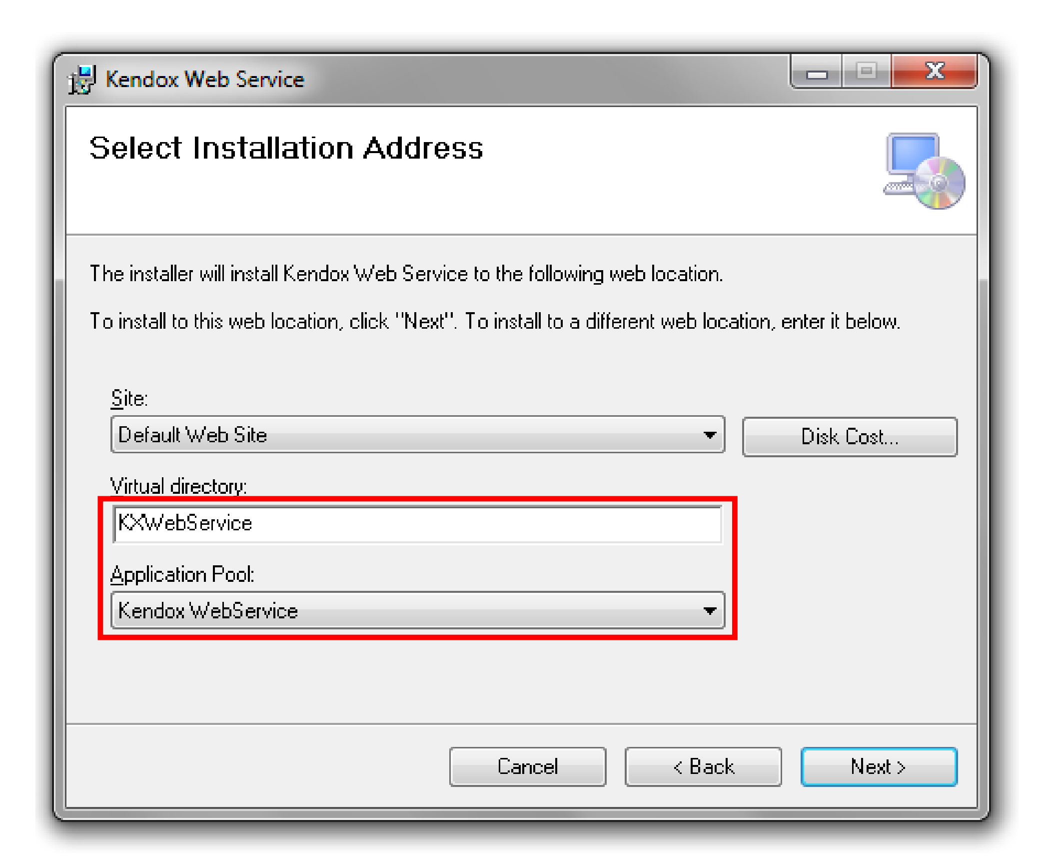


   In diesem Fall muss der Benutzer gewechselt werden (z. B. Administrator).

   Wurde unter IIS 7 die IIS 6-Kompatibilität (siehe Kapitel „Konfiguration IIS 7") nicht installiert oder hat der angemeldete Benutzer zu wenig Rechte, erscheint folgendes Fenster:

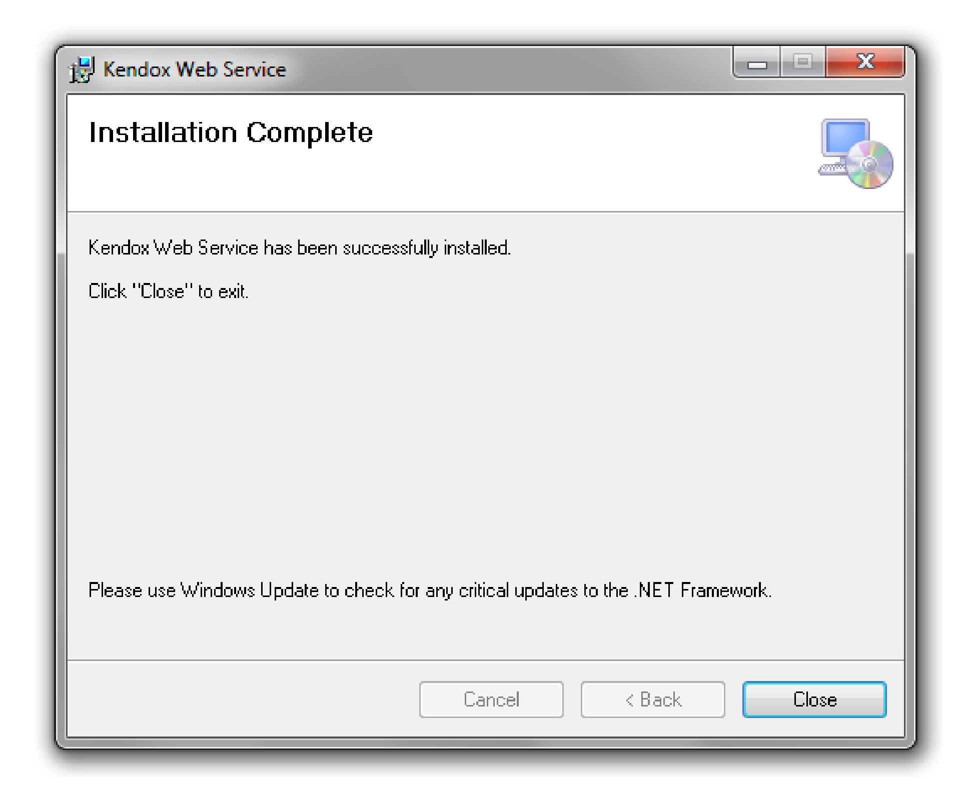


3. Webservice-Verzeichnisnamen und Application-Pool setzen:



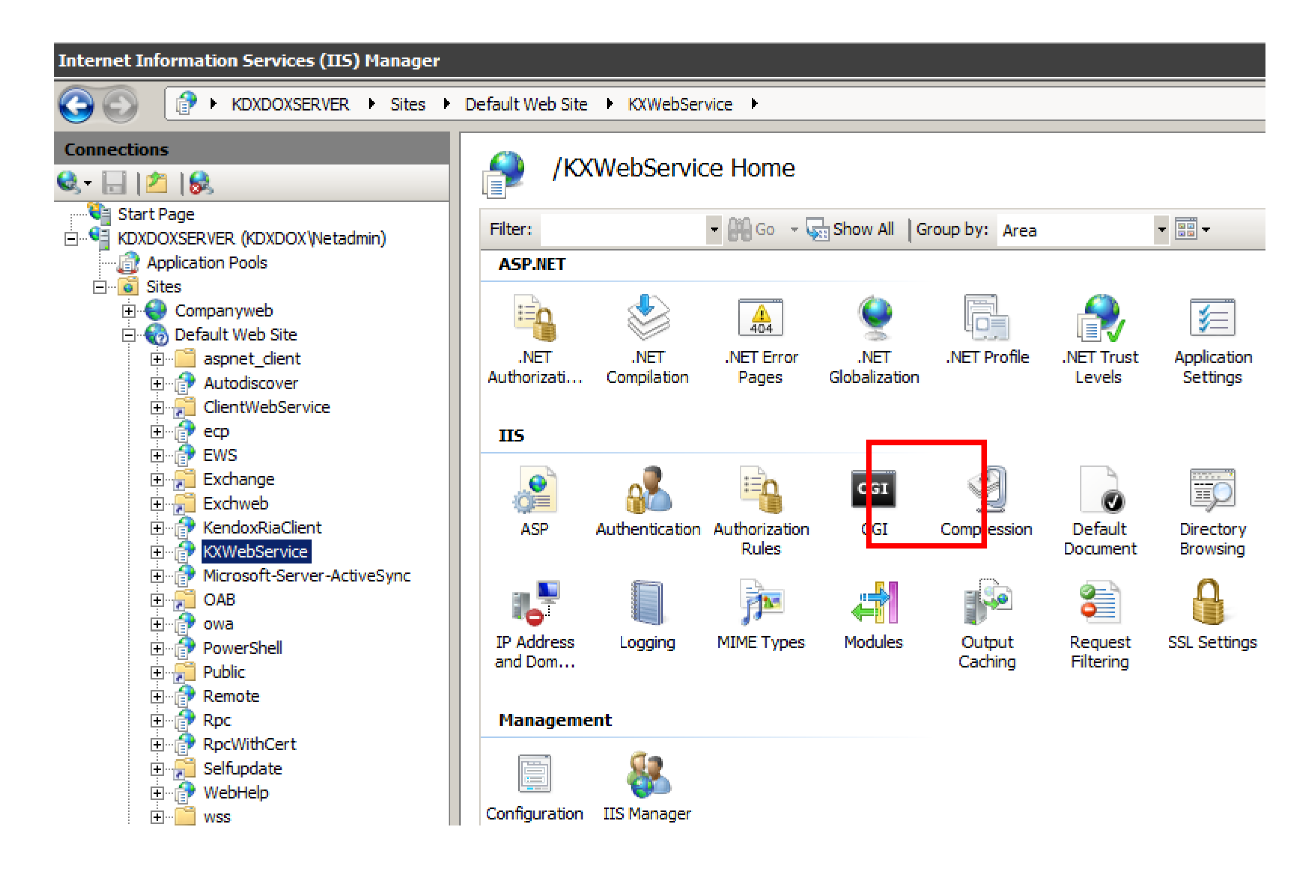
Es kann entweder ein eigener Kendox WebService Application Pool (falls erstellt) oder ein vorhandener **ASP.NET v4.0 Integrated** (Standard ohne SSO) Application Pool verwendet werden. Hierbei ist zu beachten, dass zwingend das .NET Framework 4.0 und der integrierte verwaltete Pipelinemodus verwendet werden (siehe Punkt 1).

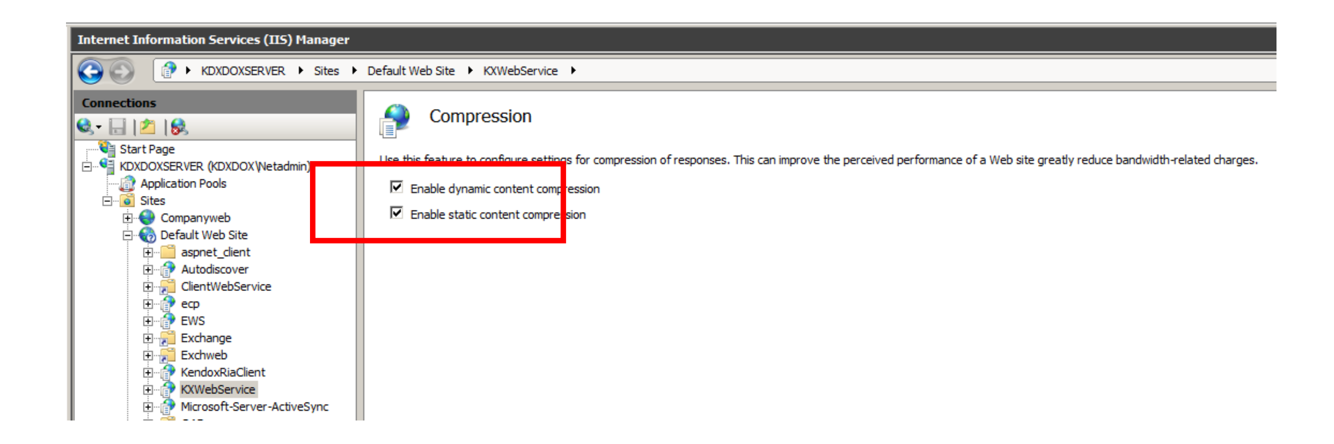
4. Im nächsten Fenster kann mit „Next >" die Installation gestartet werden. Nach erfolgreicher Installation erscheint folgendes Fenster:



9.3 Komprimierung der Datenübertragung unter IIS 7

Nach erfolgreicher Installation des Kendox WebService kann auf Stufe Web Applikation die Komprimierung der Datenübertragung aktiviert werden um die Datenübertragung bei geringen Bandbreiten zu verschnellern.





Siehe auch: http://technet.microsoft.com/de-de/library/cc753681%28v=ws.10%29.aspx

9.4 WebService Autostart Funktion im IIS

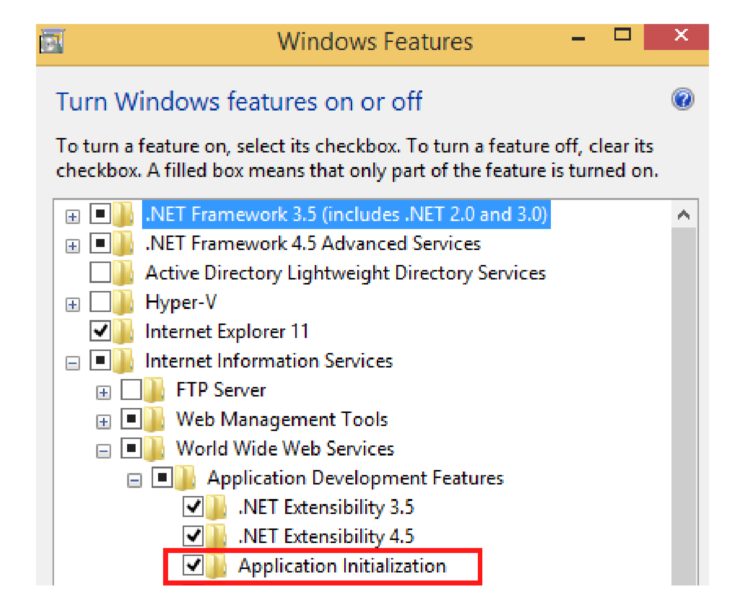
Damit eine IIS-Applikation (z.B. Kendox InfoShare WebService oder eine andere Web-Applikation) bereits beim Hochfahren oder Neustart (IISReset) des IIS gestartet wird und nicht erst bei beim Aufruf der ASMX/ASPX-Seite, müssen folgende Vorkehrungen getroffen werden:

- Windows Features:
  Das Windows-Feature „Anwendungsinitialisierung“ muss aktiviert sein
- IIS Manager:
  Der Application-Pool, in dem der WebService, bzw. die Web-Applikation läuft, muss auf „AlwaysRunning“ und das Leerlauftimeout auf „0“ gesetzt
  werden.
  Die Web-Anwendung muss auf „Vorabladen aktiviert“ auf „True“ gesetzt werden
- Web.Config.xml:
  In der web.config Datei des zu startenden WebServices/WebAnwendung, muss die ASMX/ASPX-Seite eingetragen werden, welche beim Start des IIS aufgerufen werden soll

Diese Autostart bzw. Preloaded WebService-Funktion steht ab IIS 7.5 (Win 2008R2 Server) zur Verfügung. Somit ebenfalls in Win2012-Server, Windows 7 sowie Windows 8 und 8.1. Exemplarisch wird im Folgenden die Konfiguration unter IIS 8 erklärt.

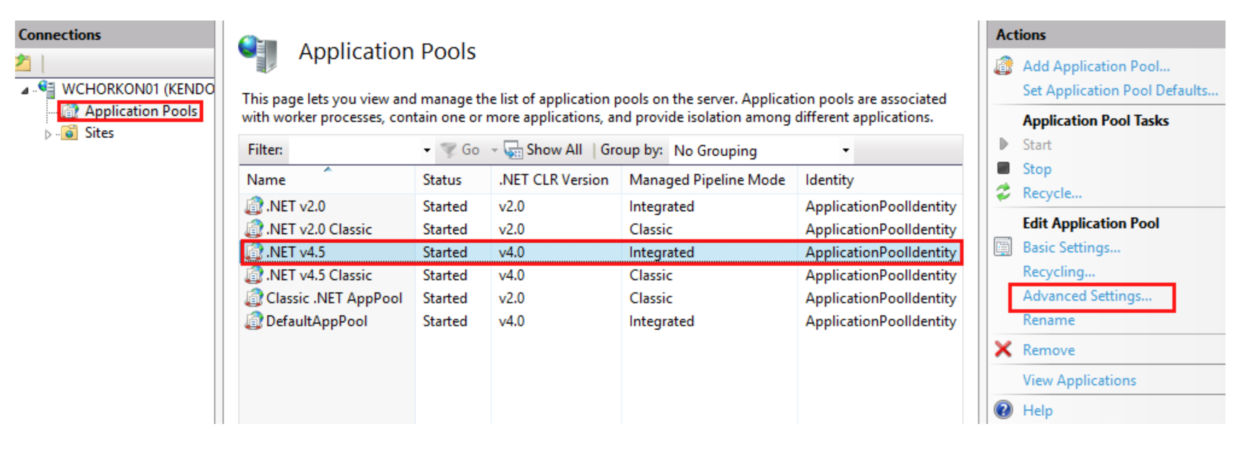
9.4.1 Windows Features

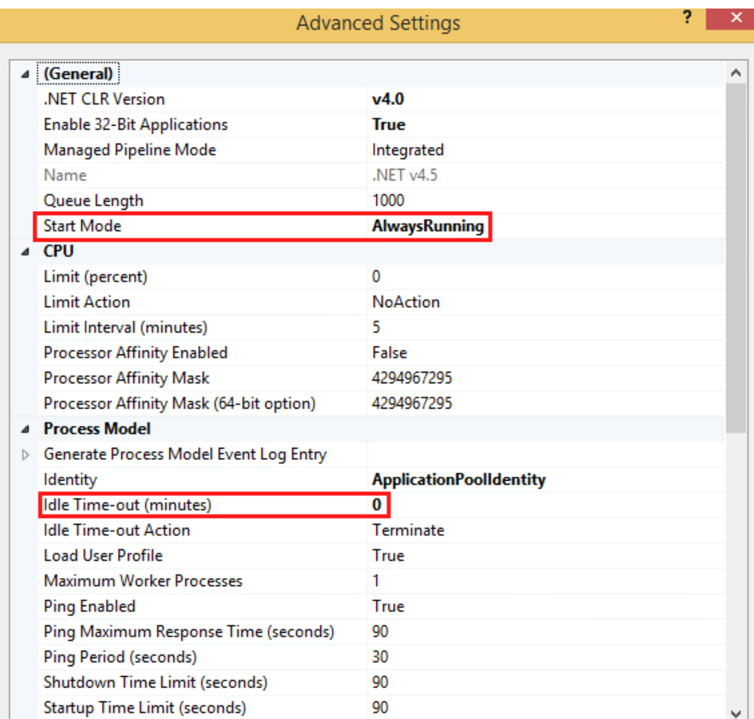
Über die Windows Features muss die Checkbox „Anwendungsinitialisierung“ aktiviert werden



9.4.2 IIS-Manager Settings

Applicationpool Settings

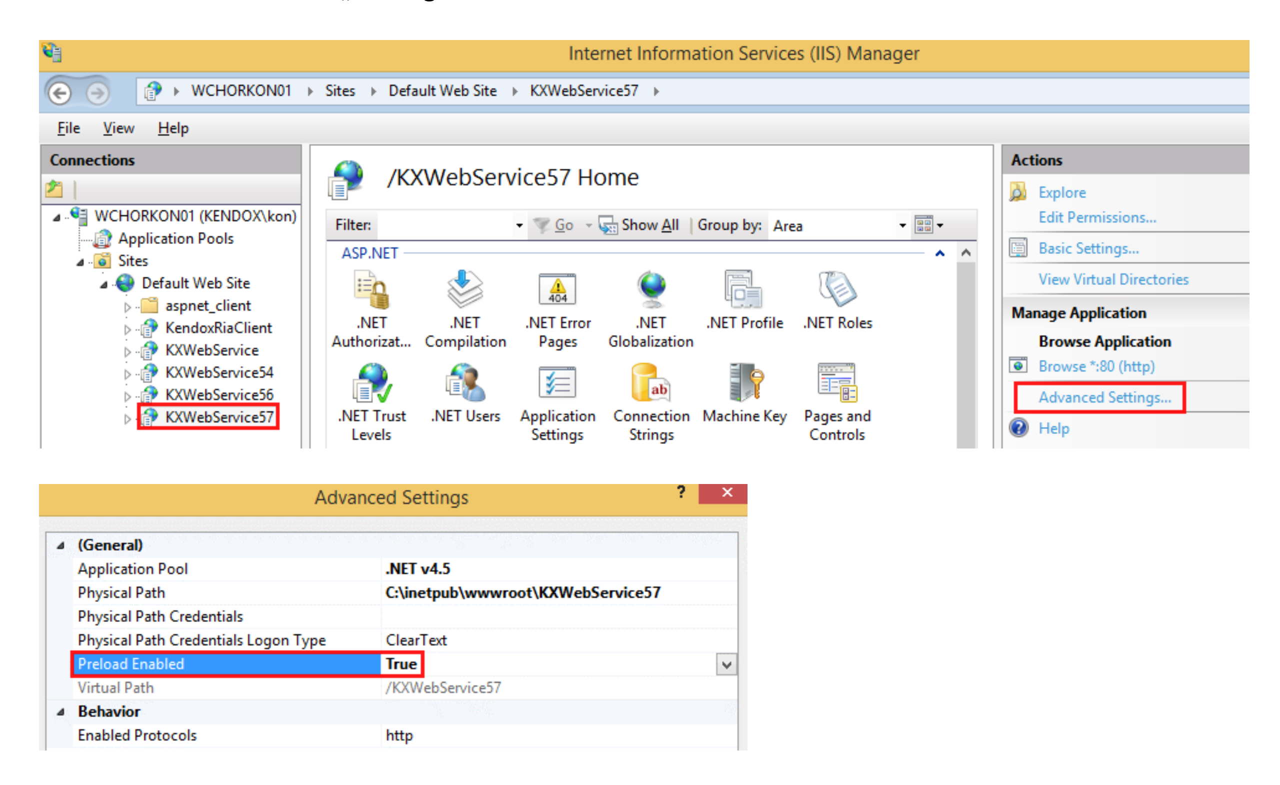




Der ***„Leerlauftimeout (Minuten)“ (Idle)*** muss ebenso auf 0 gesetzt werden.
Ansonsten wird der WebService/WebAnwendung nach der definierten Zeit, wenn keine Aktivitäten festgestellt wurden, heruntergefahren und gestartet.

WebService Advanced Settings

In den Advanced Settings des verwendeten Webservice muss das Feature „Vorladen aktivieren“ auf den Wert „true“ gesetzt werden.



9.4.3 Web.config.xml

Der Tag <applicationInitialization> muss in der web.config.xml Datei ergänzt werden.

```
<system.webServer>
    <applicationInitialization>
        <add initializationPage="kxwebservice57.asmx"/>
    </applicationInitialization>
    <!-- Allow content up to x bytes (usually set the maxRequestLength in bytes) -->
    <security>
      <requestFiltering>
          <requestLimits maxAllowedContentLength="419430400" />
    <fileExtensions allowUnlisted="false" >
      <add fileExtension=".asmx" allowed="true"/>
    </fileExtensions>
        </requestFiltering>
    </security>
</system.webServer>
```



Hinweis: zur ASMX/ASPX-Seite können ebenfalls URL-Parameter mitgegeben werden. Somit wird nicht nur der WebService, sondern auch bereits schon mal ein Logon initialisiert. Z.B.:

```
<applicationInitialization>
      <add initializationPage="kxwebservice.asmx/Logon?serverName=localhost&amp;
       serverPort=23451&amp;userName=dciadmin&amp;userPassword=&amp;
       currentCulture=de-CH&amp;currentUICulture=de-CH" />
</applicationInitialization>
```

Damit der Aufruf der „initalizationPage=…“ mit einem Funktionsaufruf funktioniert, muss das „HttpGet“ Protokoll in der Web.config Datei aktiviert werden.

```
<webServices>
    <protocols>
        <!-- Only allow soap communication -->
        <!--<remove name="HttpPost"/>-->
        <!-- <remove name="HttpGet"/>-->
        <!-- Add the next two lines to use url-parameter to invoke the web service...-->
        <add name="HttpGet" />
<add name="HttpPost" />
<remove name="HttpSoap12" />
        <add name="HttpSoap" />
    </protocols>
</webServices>
```

10 Konfiguration von Kendox WebService

10.1 Konfigurationsdatei „ConnectionPoolSettings.xml“

Die Hauptkonfigurationsdatei befindet sich im absoluten Webservice-Verzeichnis, in dem der Webservice installiert wurde (z. B. „C:\inetpub\wwwroot\KXWebService\“):

```
<?xml version="1.0"?>
<Configuration xmlns="http://www.kendox.com/ConnectionPool">
    <ConnectionPoolConfigurationSettings xmlns="">
        <MinPoolSize>3</MinPoolSize>
        <MaxPoolSize>10</MaxPoolSize>
        <UserCredentialFileName>ConnectionPoolCredentials.xml</UserCredentialFileName>
        <UserCredentialLifetime>90</UserCredentialLifetime>
        <WrapperConfigFileName>config.xml</WrapperConfigFileName>
        <WrapperPluginDirectory></WrapperPluginDirectory>
        <TempDirectory>KXWebServiceTemp</TempDirectory >
        <GarbageCollectorInterval>30</GarbageCollectorInterval>
        <TransactionLifeTime>60</TransactionLifeTime>
        <ConverterWebServiceUrl></ConverterWebServiceUrl>
        <KeySize>256</KeySize>
```

```
        <KeyFileName>XMLEncryptionData.key</KeyFileName>
        <OverlayListFileName>OvlerayList.xml</OverlayListFileName>
    </ConnectionPoolConfigurationSettings>
</Configuration>
```

*Die schwarz markierten Tags können angepasst werden.

Bis Kendox WebService Version 4.0.15 wurden im ConnectionPoolSettings.xml die Einträge <FileExportDirectory>, <FileImportDirectory>, <AnnotationTemplatesDirectory>, <DockingLayoutTemplateDirectory> und <DockingLayoutDirectory> gepflegt. Diese Einträge wurden ab Kendox WebService 4.0.16 entfernt und durch den Eintrag <TempDirectory> ersetzt.

Innerhalb des <TempDirectory> werden die Unterverzeichnisse „Export“, „Import“, „AnnotationTemplates“, „DockingLayouts“ und „DockingLayouts/Templates“ automatisch durch den Kendox WebService angelegt. Auf das <TempDirectory> benötigt der Benutzer, der den Kendox WebService ausführt, Schreibrechte.



Hinweis: Allfällig vorhandene AnntoationTemplates und DockingLayouts müssen manuell in die neuen Verzeichnisse übertragen werden.

Wird im <TempDirectory> ein relativer Pfad angegeben (z.B. „KXWebServiceTemp“), so wird dieses Verzeichnis relativ zum Installationspfad des Kendox WebServices gesucht (z.B. „C:\inetpub\wwwroot\KXWebService\KXWebServiceTemp“).

Wird ein expliziter Pfad hinterlegt (z.B. „C:\KxWebServiceTemp“), so wird exakt das <TempDirectory> gesucht.

Ab Version 4.0.16 werden die Dateien aus dem Tag „<UserCredentialFileName>“ und „<KeyFileName>“, sowie weitere Dateien im relativen <TempDirectory> abgelegt. Ist kein relatives <TempDirectory>-Verzeichnis eintgetragen, werden die Dateien im relativen Verzeichnis „KxWebServiceTemp“ innerhalb des Kendox WebService Installationsverzeichnisses abgelegt. Auf dieses Verzeichnis benötigt der Benutzer, der den Kendox WebService ausführt, Schreibrechte.

Um Dateien mit der WebService-Methode „GetDocumentFileSimple(..)“ zu exportieren, muss der Webservice unter einem Benutzer laufen, der auf das Zielverzeichnis „exportPath“ genügend Zugriffsrechte hat; das Zielverzeichnis muss existieren (z. B. exportPath="C:\Export\“ oder exportPath="\\myServer\sharedfolder\“).



Hinweis: Lokale Verzeichnisse wie zum Beispiel das Verzeichnis „C:\Export\“ aus dem obigen Beispiel beziehen sich immer auf ein lokales Verzeichnis, auf dem der WebService installiert ist.

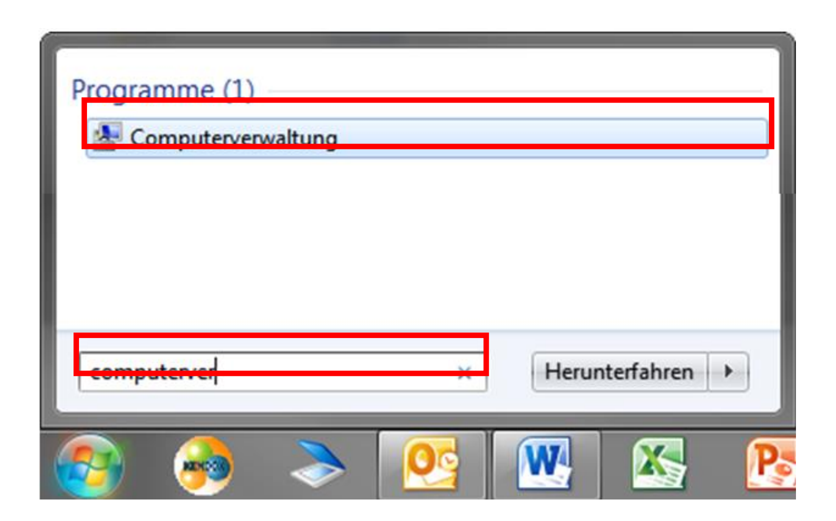
10.2 AnwendungsPool für den WebService (IIS 7.x)

Überprüfung des Anwendungspools

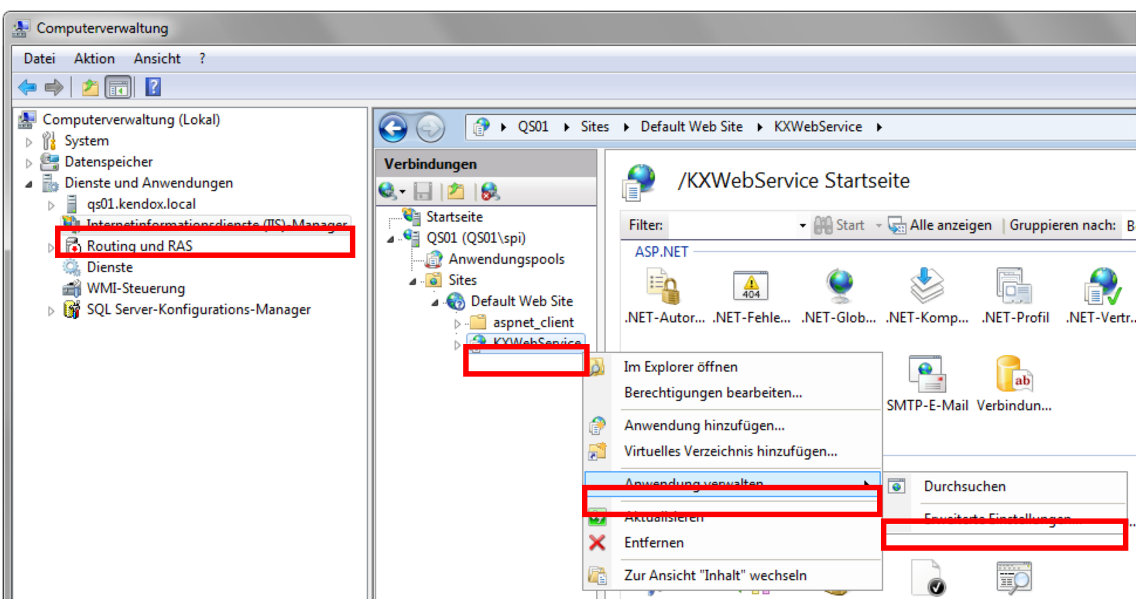
Im IIS 7.x muss der Anwendungspool, unter dem der WebService läuft, wie folgt überprüft / verändert werden:

1. Zu Beginn muss die Computerverwaltung geöffnet werden.

   „Start“ → Nach „Computerverwaltung“ suchen und öffnen:



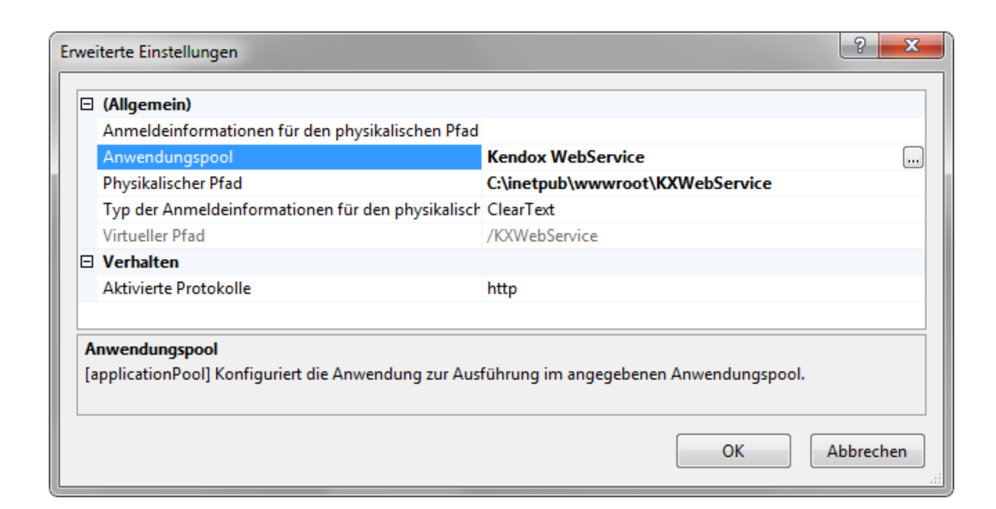
2. Nun muss überprüft werden, ob der gewünschte Applikationspool während der Installation korrekt übernommen wurde. Hierzu muss mit einem Rechtsklick in der Computerverwaltung auf das Installationsverzeichnis des Kendox WebService (standardmässig „KXWebService“) unter „Anwendung verwalten“ → „Erweiterte Einstellungen…“ gewählt werden.

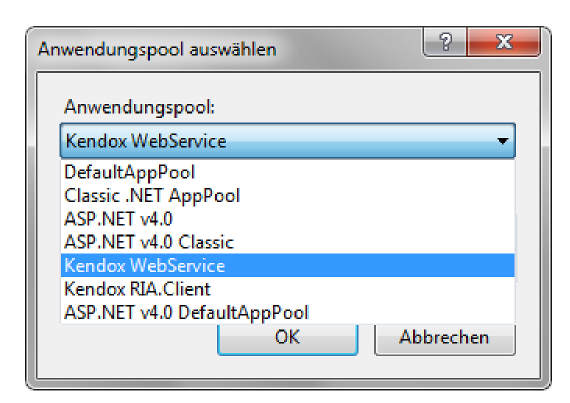


Beim neu geöffneten Fenster muss der Wert von „Anwendungspool“ überprüft werden.

Wurde ein eigener Applikationspool erstellt, sollte hier der definierte Applikationspool-Name stehen (hier „Kendox WebService“) . Falls ein bestehender Applikationspool übernommen

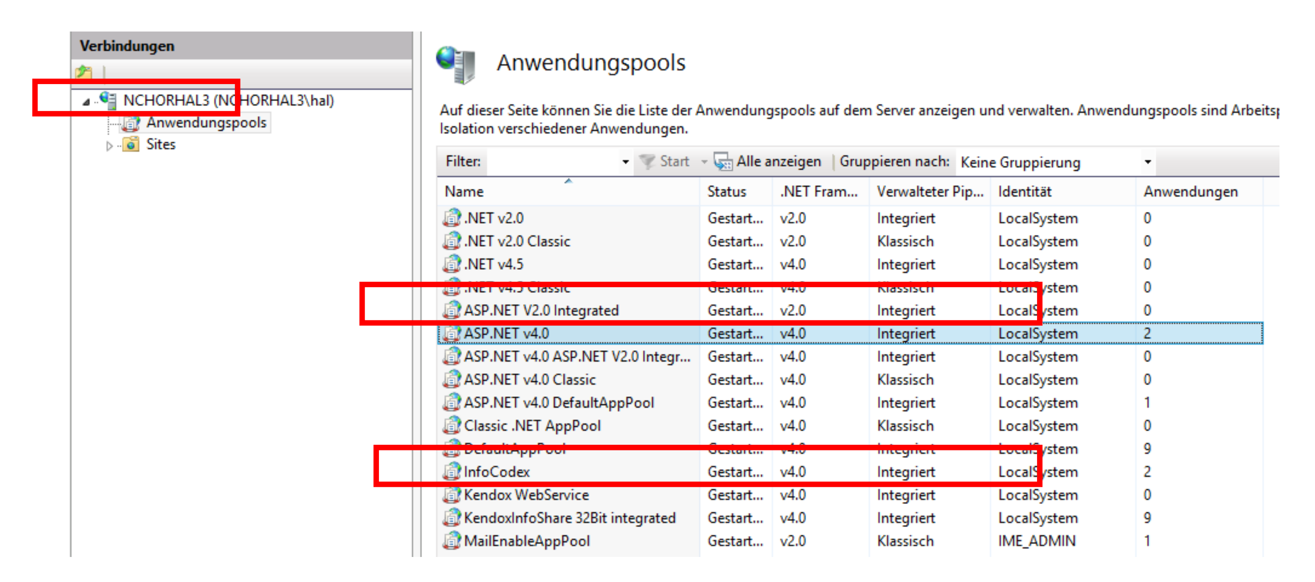
wurde, sollte überprüft werden, ob „**ASP.NET v4.0 integrated**“ ausgewählt ist. Falls nicht, kann mit dem Button „..." der Anwendungspool ausgewählt werden (siehe rote Markierung).



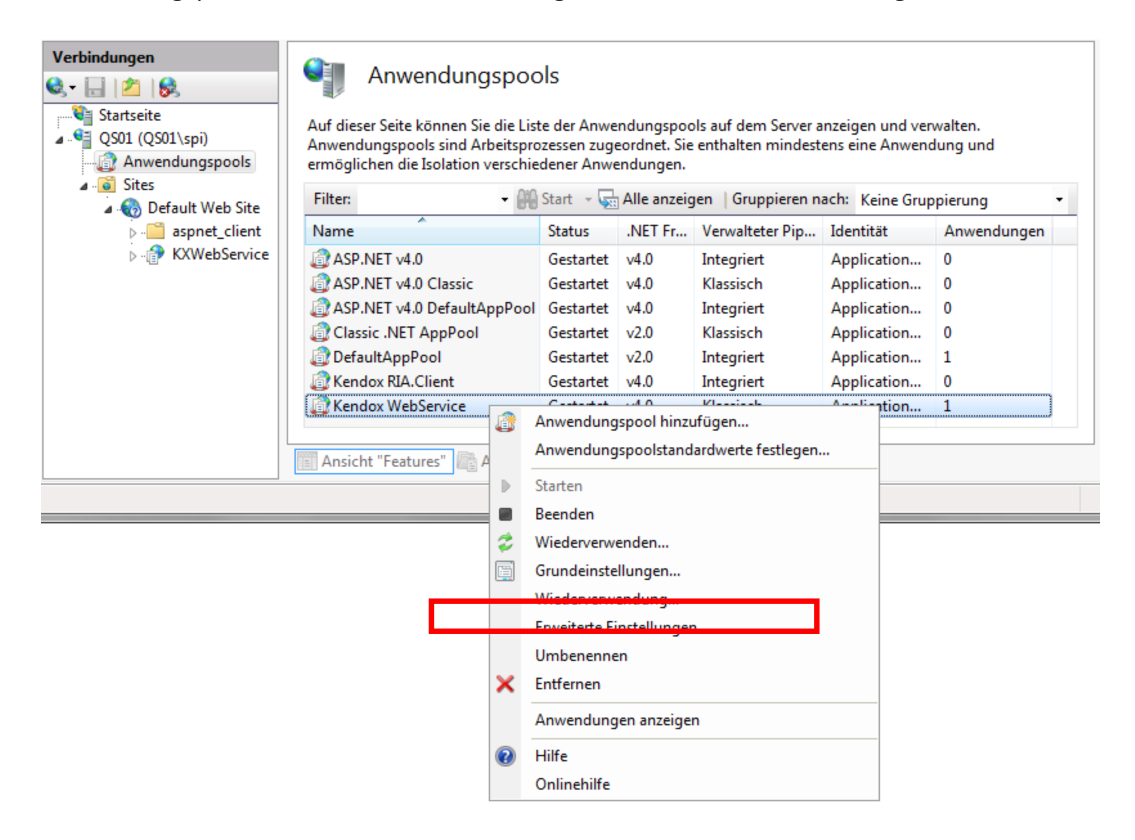


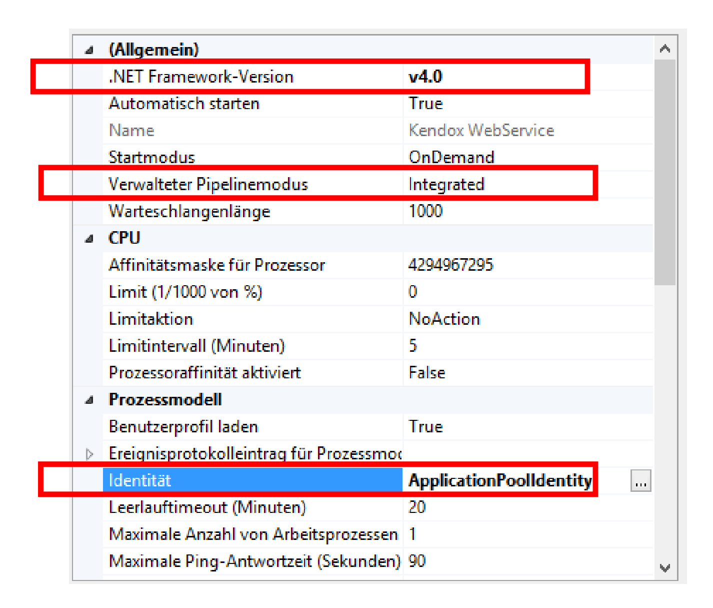
Konfiguration des Anwendungspools

Der für Kendox WebService verwendete Anwendungspool muss auf eine korrekte Installation überprüft werden, damit bei der späteren Verwendung keine Probleme auftreten. Hierzu muss in der Computerverwaltung unter „Dienste und Anwendungen“ → Internetinformationsdienste (IIS)-Manager → [SERVERNAME] → „Anwendungspools“ der entsprechende Applikationspool ausgewählt werden (eigener, z. B. „Kendox WebService“ oder bereits existierender „ASP.NET v4.0 integrated“):



Mit einem Rechtsklick auf den entsprechend für Kendox WebService verwendeten Anwendungspool → „Erweiterte Einstellungen“ wird ein neues Fenster geöffnet:





Folgende Punkte sind im Fenster „Erweiterte Einstellungen“ zu prüfen:

- Falls ein 64-Bit System eingesetzt wird, muss der Punkt „32-Bit Anwendung aktivieren“ auf „True“ gesetzt sein → Bei einem 32-bit System ist dieser Punkt nicht vorhanden
- Verwalteter Pipelinemodus muss auf **Integrated** stehen; gegebenenfalls muss dieser gesetzt werden
- Es muss sichergestellt werden, dass die „Identität“ auf **ApplicationPoolIdentity** gesetzt ist; gegebenenfalls muss diese gesetzt werden

Die Änderungen sind mit „OK“ zu bestätigen.

10.3 Mögliche Probleme bei IIS 6 und IIS 7

Code-Definitionen

Minimale Anzahl Verbindungen

<MinPoolSize>3</MinPoolSize>

- ➔ Definiert die minimale Anzahl der offenen Verbindungen zum InfoShare-Server
- ➔ Wird im Moment nicht verwendet

Maximale Anzahl Verbindungen

<MaxPoolSize>10</MinPoolSize>

- ➔ Definiert die maximale Anzahl der offenen Verbindungen zum InfoShare-Server
- ➔ Bedingung: [MinPoolSize] <= [MaxPoolSize]

Speicherort der Benutzerauthentifizierungen

<UserCredentialFileName>ConnectionPoolCredentials.xml</UserCredentialFileName>

- ➔ Speicherort der Benutzerauthentifizierungen (wichtige Daten sind verschlüsselt); Diese Datei wird im <TempDirectory>-Pfad gespeichert. Ist das <TempDirectory> KEIN relativer Pfad, wird die Datei im relativen Verzeichnis „KxWebServiceTemp" innerhalb des Kendox WebService-Installationsverzeichnisses gespeichert (z.B. „C:\inetpub\wwwroot\KXWebService\KXWebServiceTemp"). Der Benutzer, unter dem der WebService läuft, muss Schreiberechte auf das Verzeichnis besitzen, ansonsten gehen die Verbindungen bereits angemeldeter Benutzer bei einem WebService-Neustart verloren.



Hinweis: Kann die Datei aus dem Konfigurations-Tag „UserCredentialFileName" beim Herunterfahren des WebServices nicht geschrieben werden, z. B. weil das Schreibrecht für den Kendox WebService fehlt, werden temporäre Dateien und Verzeichnisse aus den Konfigurations-Tags „<TempDirectory>" nicht gelöscht und der GarbageCollector funktioniert nicht korrekt. Betroffen sind auch Dateien, welche über Transaktionen importiert/exportiert werden.

Timeout einer Session-ID

<UserCredentialLifetime>10</UserCredentialLifetime>

- ➔ Timeout einer Session-ID in Minuten
- ➔ Wurde die Session-ID eine Anzahl [UserCredentialLifetime] Minuten nicht mehr verwendet, wird sie ungültig und der Benutzer muss sich erneut anmelden

DCIS-Wrapper-Konfigurationsdatei

<WrapperConfigFileName>config.xml</WrapperConfigFileName>

- ➔ Speicherort der DCISWrapper-Konfigurationsdatei
- ➔ Befindet sich standardmässig im Root-Verzeichnis des WebServices

Verzeichnis des DCIS-Wrapper-Plugins

<WrapperPluginDirectory></WrapperPluginDirectory>

- ➔ Speicherort der InfoShare-Plugins für WebService
- ➔ Wird zurzeit nicht verwendet

Temporäres Verzeichnis

<TempDirectory>KXWebServiceTemp</TempDirectory>

- ➔ Temporäres Verzeichnis für Dateien, die aus InfoShare exportiert werden
- ➔ Dieses Verzeichnis wird auch für temporäre Dateien bei Download-Transaktionen (z. B. Download-Junks) verwendet
- ➔ Innerhalb des Verzeichnisses werden automatisch weitere Verzeichnisse angelegt
  - Import: Verzeichnis mit allen Dokumenten die importiert wurden
  - Export: Verzeichnis mit allen Dokumenten die für die Anzeige, Druck, usw. benötigt wurden
  - DockingLayouts: Kendox RIA.Client Fenstereinstellungen pro Benutzer
  - DockingLayouts/Templates: Vorlagen für die Fenstereinstellungeen
  - AnnotationTemplates: Stempelvorlagen



Hinweis: Kann die Datei aus dem Konfigurations-Tag „UserCredentialFileName“ beim Herunterfahren des WebServices nicht geschrieben werden, z. B. weil das Schreibrecht für den Kendox WebService fehlt, werden temporäre Dateien und Verzeichnisse aus den Konfigurations-Tags „<TempDirectory>“ nicht gelöscht und der GarbageCollector funktioniert nicht korrekt. Betroffen sind auch Dateien, welche über Transaktionen importiert/exportiert werden.

GarbageCollector-Intervall

<GarbageCollectorInterval>10</GarbageCollectorInterval>

- ➔ Intervall in Minuten, in dem der „GarbageCollector“ wiederholt gestartet wird. Der „GarbageCollector“ löscht abgelaufene Benutzer („UserGuids“), temporäre Dateien und Verzeichnisse und schliesst nicht mehr gebrauchte Verbindungen zum InfoShare-Server

Transaktions-Timeout

<TransactionLifeTime>60</TransactionLifeTime>

- ➔ Zeit in Minuten, nachdem eine Transaktion nach dessen letzten Zugriff gelöscht wird
- ➔ Die Transaktionen werden vom „GarbageCollector“ aussortiert
- ➔ Transaktionen, welche noch nicht abgeschlossen sind und länger als z. B. 60 Minuten nicht mehr verwendet wurden, werden auch gelöscht

Konvertierungs-WebService-Url (Kendox ConverterService)

<ConverterWebServiceUrl></ConverterWebServiceUrl>

- ➔ Sollen Dokumente beim Export mit der Methode „GetDocumentFileConverted“ in ein anderes Format konvertiert werden, muss die WebService-URL angegeben werden, auf dem der „Kendox ConverterService“ installiert ist (z. B. http://localhost/kxConverterService/kxConverterService.asmx)
- ➔ Ist das Tag leer, steht keine Dokumentkonvertierung für Kendox WebService zur Verfügung; die Methode „GetDocumentFileConverted“ kann dann nicht verwendet werden
- ➔ Details über die Konfiguration bzw. die Installation des Kendox ConverterService sind im gleichnamigen Benutzerhandbuch beschrieben

---



Hinweis: Ist eine URL für den Kendox ConverterService definiert, überprüft Kendox WebService beim Start, ob die URL erreichbar ist. Falls eine falsche URL angegeben wurde bzw. der Kendox ConverterService nicht läuft, kann der Kendox WebService nicht gestartet werden und eine Fehlermeldung wird ausgegeben.

Key-Size

<KeySize>256</KeySize>

- ➔ Schlüsselgrösse, die für die Verschlüsselung in den Dateien „ConnectionPoolCredentials.xml“ und „UpDownloadManagerTransactions.xml“ verwendet wird
- ➔ Mögliche Werte sind 128 und 256; je grösser der Schlüssel, desto sicherer die Verschlüsselung

KeyFile-Name

<KeyFileName>XMLEncryptionData.key</KeyFileName>

- ➔ In dieser Datei wird der generierte Schlüssel mit der Länge „KeySize“ abgelegt; diese Datei wird beim Starten des WebServices generiert, falls sie noch nicht vorhanden ist
- ➔ In dieser Datei darf nichts verändert werden, da ansonsten die gespeicherten Benutzer und Transaktionen nicht mehr entschlüsselt werden können
- ➔ Diese Datei wird im <TempDirectory>-Pfad gespeichert. Ist das <TempDirectory> KEIN relativer Pfad, wird die Datei im relativen Verzeichnis „KxWebServiceTemp“ innerhalb des Kendox WebService-Installationsverzeichnisses gespeichert (z.B. „C:\inetpub\wwwroot\KXWebService\KXWebServiceTemp“). Der Benutzer, unter dem der WebService läuft, muss Schreiberechte auf das Verzeichnis besitzen.

10.4 Konfigurationsdatei „URLEncryptionSettings.xml“

Diese Konfigurationsdatei wird für die WebService-Methoden „EncryptURL“ und „DecryptURL“ verwendet, um URL-Integrationsaufrufe zu verschlüsseln bzw. entschlüsseln.

Die Konfigurationsdatei befindet sich im absoluten Webservice-Verzeichnis, in dem der Webservice installiert ist (z. B. „C:\inetpub\wwwroot\KXWebService\“):

```
<?xml version="1.0"?>
<Configuration xmlns="http://www.kendox.com/URLEncryption">
	<URLEncryptionConfigurationSettings xmlns="">
		<Lifetime>60</Lifetime>
		<KeySize>256</KeySize>
		<KeyFileName>URLEncryptionData.key</KeyFileName>
	</URLEncryptionConfigurationSettings>
</Configuration>
```

*Die schwarz markierten Tags können angepasst werden.

Code-Definitionen

LifeTime

```
<Lifetime>60</Lifetime>
```

- ➔ Zeitspanne in Sekunden, in der eine verschlüsselte URL wieder entschlüsselt werden kann

Key-Size

```
<KeySize>256</KeySize>
```

- ➔ Schlüsselgrösse, die für die Verschlüsselung der WebService-Methoden verwendet wird
- ➔ Mögliche Werte sind 128 und 256; je grösser der Schlüssel, desto sicherer ist die Verschlüsselung

KeyFile-Name

```
<KeyFileName>XMLEncryptionData.key</KeyFileName>
```

- ➔ In dieser Datei wird der generierte Schlüssel mit der Länge „KeySize“ abgelegt; diese Datei wird beim Starten des WebServices generiert, falls sie noch nicht vorhanden ist
- ➔ In dieser Datei darf nichts verändert werden
- ➔ Die Datei wird in das <TempDirectory>-Verzeichnis, welches in der Datei „ConnectionPoolSettings.xml“ definiert ist abgelegt. Ist jedoch in der Pfad des <TempDirectory> explizit, wird die Datei ins relative Verzeichnis „KxWebServiceTemp“ innerhalb des Installationsverzeichnisses des Kendox WebServices abgelegt (z.B. „C:\inetpub\wwwroot\KXWebService\KXWebServiceTemp“). Auf dieses Verzeichnis benötigt der Benutzer, der den Kendox WebService ausführt, Schreibrechte.
- ➔ Ist das Tag „KeyFileName“ in den Konfigurationsdateien „ConnectionPoolSettings.xml“ und „URLEncryptionSettings.xml“ gleich, muss die „KeySize“ auch gleich sein, da sonst unterschiedliche Schlüsselgrössen zu Problemen führen, da die gleiche „KeyFileName“ verwendet wird; in einem solchen Fall muss „KeyFileName“ unterschiedlich sein

11 Single-Sign-On (ADS-Integration)

Die Einstellungen in diesem Kapitel müssen nur dann vorgenommen werden, wenn Kendox WebService mit „Single-Sign-On“ (kurz SSO) betrieben werden soll.

Aus den Überschriften der folgenden Unterkapitel kann die IIS-Version entnommen werden, für die das Unterkapitel gültig ist. Soll z. B. ein IIS 6.x konfiguriert werden, müssen alle Anweisungen in den Unterkapiteln ausgeführt werden, die in der Überschrift „IIS 6.x“ beinhalten.

11.1 Webservice bei Verwendung mit SSO

Der WebService bei Verwendung von SSO (Windows Authentication) muss in einem Application Pool im "Classic Pipeline Mode" (nicht „Integriert“) laufen. Ansonsten (ohne SSO) ist „Integriert“ der richtige Modus. Beim RIA.Client ändert sich nichts da dieser immer Integriert laufen.

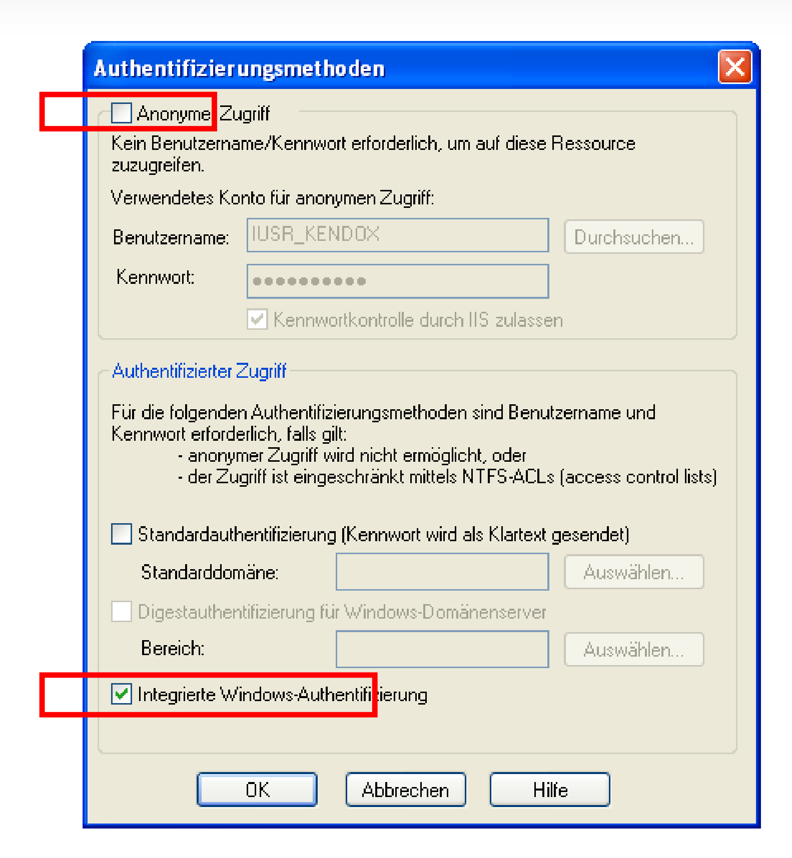
11.2 Authentifizierungsmethoden unter IIS 5.x/6.x

Im IIS 5.x/6.x müssen der „Anonyme Zugriff“ deaktiviert und die „Integrierte Windows-Authentifizierung“ aktiviert werden. Die Einstellungen sind im Fenster „Authentifizierungsmethoden“ zu finden.

In das Fenster „Authentifizierungsmethoden“ gelangt man über „Start“ → „Eigenschaften“ → „Systemsteuerung“ → „Verwaltung“ → „Internet-Informationsdienste“ → [SERVER] → „Websites“ → „Standardwebsite“ → Rechtsklick auf „KxWebService“ → „Eigenschaften“ → „Verzeichnissicherheit“ → „Steuerung des anonymen Zugriffs und der Authentifizierung“.

Dies bewirkt, dass sich der Benutzer am ADS resp. am WebServer anmelden muss, sofern der WebServer die Benutzerinformationen nicht vom Internet-Browser übernehmen kann.

Nach erfolgter Anmeldung läuft der IIS-Prozess unter dem angemeldeten Benutzer.


Authentifizierungsmethoden
Anonymer Zugriff
Kein Benutzername/Kennwort erforderlich, um auf diese Ressource zuzugreifen.
Verwendetes Konto für anonymen Zugriff:
Benutzername:
IUSR_KENDOX
Durchsuchen...
Kennwort:
Kennwortkontrolle durch IIS zulassen
Authentifizierter Zugriff
Für die folgenden Authentifizierungsmethoden sind Benutzername und Kennwort erforderlich, falls gilt:
- anonymer Zugriff wird nicht ermöglicht, oder
- der Zugriff ist eingeschränkt mittels NTFS-ACLs (access control lists)
Standardauthentifizierung (Kennwort wird als Klartext gesendet)
Standarddomäne:
Auswählen...
Digestauthentifizierung für Windows-Domänenserver
Bereich:
Auswählen...
Integrierte Windows-Authentifizierung
OK
Abbrechen
Hilfe



Hinweis: Darüber hinaus müssen in der Datei Web.config folgende Tags manuell verändert werden, da die Konfiguration im UI nicht in die Datei Web.config übernommen werden:

```
<authentication mode="Windows"/>

       <identity impersonate="true"/>
```

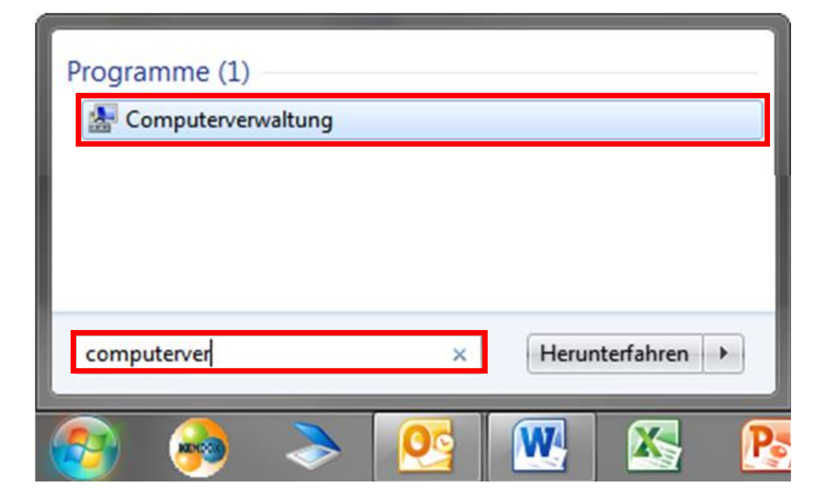
Siehe Kapitel Web.Config (IIS 5.x/6.x/7.x)

11.3 Authentifizierungsmethoden unter IIS 7.x

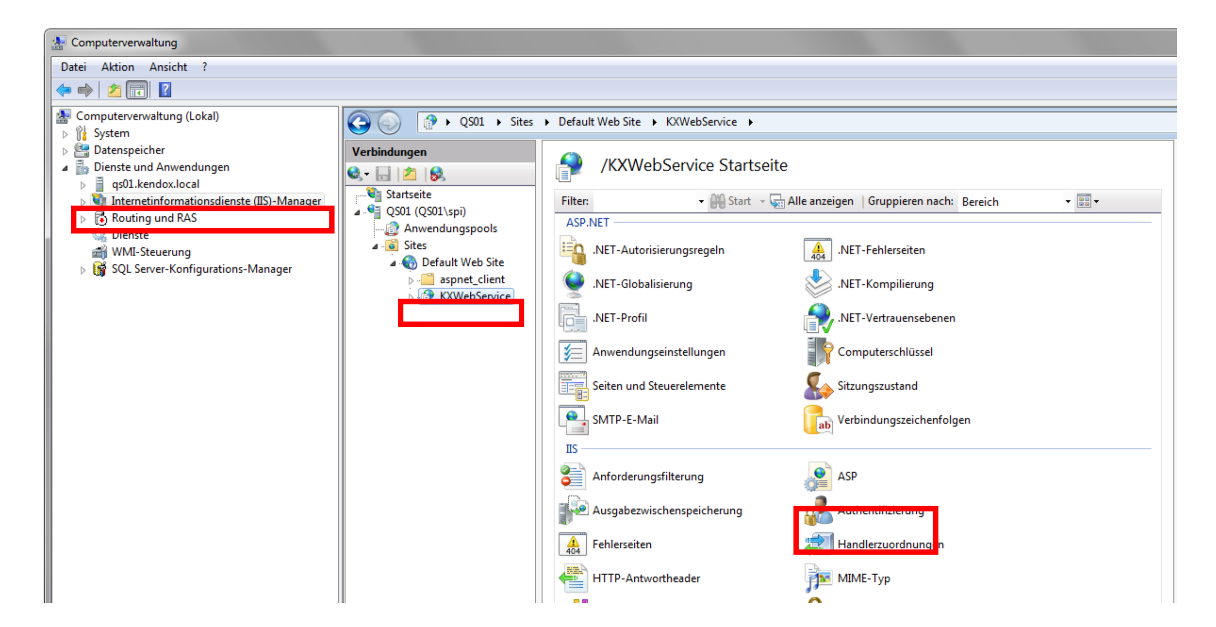
Zu beachten ist, dass bestimmte Authentifizierungsfeatures im IIS 7 installiert sein müssen, damit SSO verwendet werden kann. Die zu installierenden Features sind im Kapitel „Konfiguration IIS 7“ zu finden.

Im IIS 7.x müssen „ASP.NET-Identitätswechsel“ und „Windows-Authentifikation“ aktiviert und alle anderen Punkte deaktiviert werden. Diese sind im „Authentifizierung“-Fenster zu finden.
In das Fenster „Authentifizierung“ gelangt man auf folgenden Schritten:

1. „Start“ → Nach „Computerverwaltung“ suchen und öffnen:

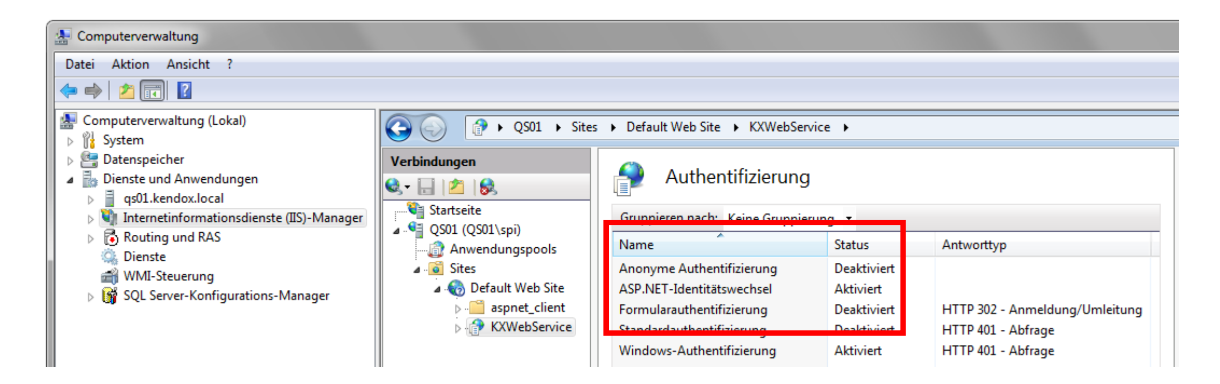


2. Nun muss in „Dienste und Anwendungen“ → „Internetinformationsdienste (IIS) –Manager“ → „Sites“ → „Default Web Site“ → Virtueller Verzeichnisname von Kendox WebService (standardmässig „KXWebService“) der Punkt „Authentifizierung“ geöffnet werden:



3. Im neu geöffneten Bereich müssen nun die folgenden Authentifizierungen aktiviert / deaktiviert sein (resp. werden):

   - Anonyme Authentifizierung: Deaktiviert
   - ASP.NET-Identitätswechsel: Aktiviert
   - Formularauthentifizierung: Deaktiviert
   - Standardauthentifizierung: Deaktiviert
   - Windows-Authentifizierung: Aktiviert



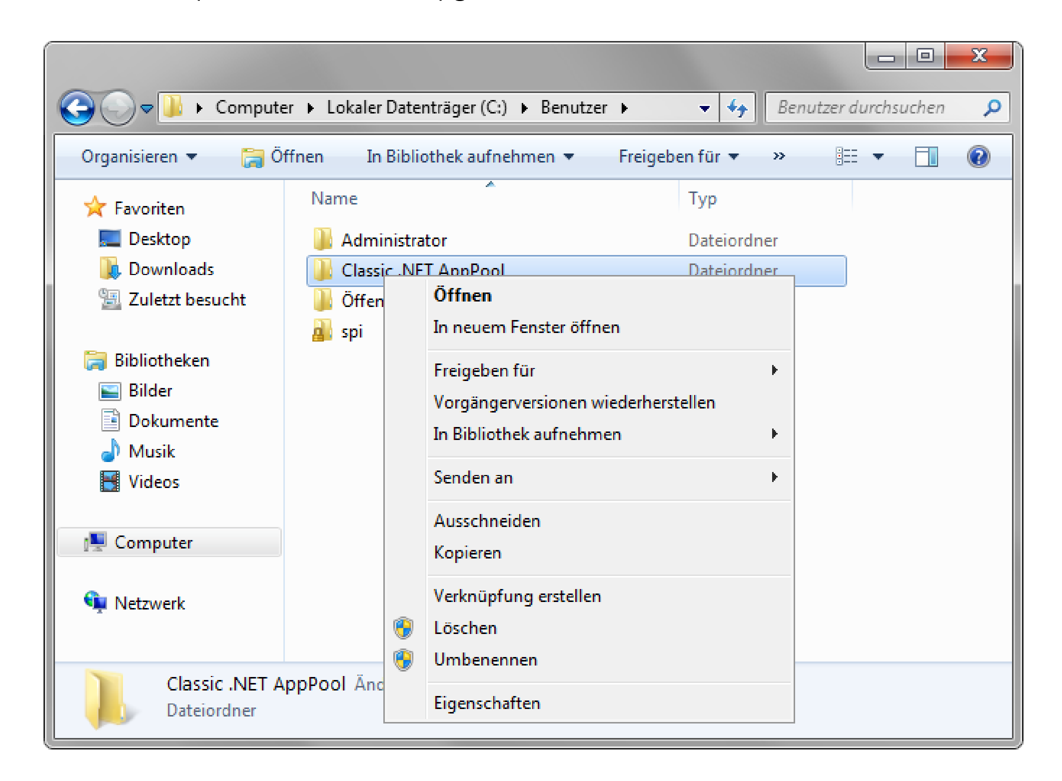
11.4 Verzeichnisberechtigungen für SSO-Benutzer (IIS 5.x/6.x/7.x)

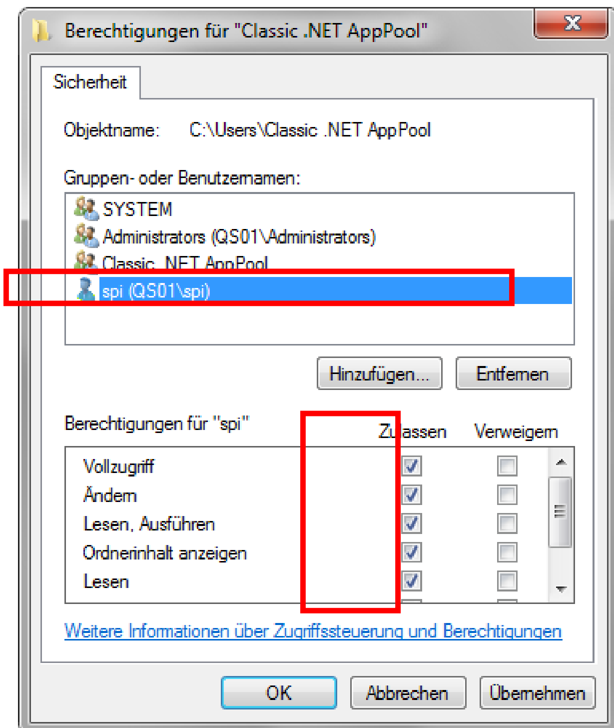
Es muss sichergestellt werden, dass die folgenden Verzeichnisse die beschriebenen Berechtigungen besitzen.

Berechtigung: Vollzugriff für alle SSO-Benutzer	
Verzeichnis	Beschreibung
Das Tag „<TempDirectory>" befindet sich in der Datei „ConnectionPoolSettings.xml".	Jeder SSO-Benutzer muss auf das angegebene Verzeichnis im Tag „TempDirectory" Vollzugriff besitzen (siehe Kapitel „Code-Definitionen" für die Tag-Beschreibungen).
C:\WINDOWS\Microsoft.NET\Framework\ v4.0.30319\ Temporary ASP.NET Files\	Da Kendox WebService beim ersten Start kompiliert wird, muss der angemeldete SSO-Benutzer auf das Microsoft.NET-Framework (temporäres Verzeichnis vom .NET Framework) Vollzugriff haben.
Berechtigung: Lese- und Schreibberechtigung für alle SSO-Benutzer	
Verzeichnis	Beschreibung
C:\WINDOWS\Temp	Damit vom Kendox WebService die Dokumente richtig exportiert werden können, muss jeder SSO-Benutzer Zugriff auf das temporäre Verzeichnis von Windows besitzen.
Berechtigung: Lese- und Schreibberechtigung für alle SSO-Benutzer	
Verzeichnis	Beschreibung
[Installationsverzeichnis von Kendox WebService]\ KXWebServiceTemp" (standardmässig unter „C:\Inetpub\wwwroot\KxWebService\KXWebServiceTemp")	Diverse temporäre Dateien (ConnectionPoolCredentials.xml, TokenEncryptionData.key, UpDownloadManagerTransactions.xml und XMLEncryptionData.key) werden ins KxWebServiceTemp-Verzeichnis. Hierfür benötigen alle Benutzer Lese- und Schreibzugriffe.
Berechtigung: Leseberechtigung für alle SSO-Benutzer	
Verzeichnis	Beschreibung

[Installationsverzeichnis von Kendox WebService]\Licenses" (standardmässig unter „C:\Inetpub\wwwroot\KxWebService\Licenses")	Alle SSO-Benutzer müssen auf folgendes Verzeichnis und den darunterliegenden Verzeichnissen und Dateien Lesezugriff besitzen.

Um Berechtigungen auf ein bestimmtes Verzeichnis bzw. auf eine bestimmte Datei zu verändern, muss ein Rechtsklick auf das entsprechende Verzeichnis / auf entsprechende Datei gemacht werden und auf „Eigenschaften“ geklickt werden. Im neu geöffneten Fenster muss in den Tab „Sicherheit“ (siehe Bildausschnitt) gewechselt werden.





Web.Config (IIS 5.x/6.x/7.x)

Um SSO zu aktivieren, müssen in der Datei „Web.Config“ (standardmässig in „C:\Inetpub\wwwroot\KxWebService“) die folgenden Einträge gesetzt werden:

```
<authentication mode="Windows">
<identity impersonate="true" />
```

Dies bewirkt, dass der IIS-Worker Prozess unter dem angemeldeten SSO-Benutzer läuft.



Hinweis: Unter IIS 7.x bewirkt die Änderung der Authentifizierung im UI auch die Änderung in der Web.config und umgekehrt. Trotzdem sollte kontrolliert werden, ob beide Stellen (UI und Web.config) richtig konfiguriert sind, falls Probleme auftreten.

---

12 Zwei-Faktor-Authentifizierung

Die in diesem Kapitel beschriebenen Einstellungen müssen vorgenommen werden, wenn Kendox Webservice mit „Zwei-Faktor-Authentifizierung“ betrieben werden soll.
Nähere Informationen und Hintergründe zur Zwei-Faktor-Authentifizierung welche ab RIA.Client Version 4.0.46 unterstützt wird, finden Sie im RIA.Client Handbuch aber Version 4.0 im Partnernet.

12.1 Anpassungen im „ConnectionPoolSettings.xml“

Das Element <TwoFactorAuthentification> wurde im „ConnectionPoolSettings.xml“ ergänzt. Hier erfolgt die Konfiguration des Zwei-Faktor-Authentifizeirung d.h. ob und wie der Email und SMS Versand erfolgt.

Überblick über das neue XML Element

```
<!-- Two Factor Authentication Section -->
<TwoFactorAuthentication>true</TwoFactorAuthentication>
<SMSProvider>aspsms.com</SMSProvider>  <!-- The sms provider. For alternative sms provider like simplesms.at please contact support@kendox.com -->
<SMSUserKey>[illegible]</SMSUserKey>      <!-- User key of the sms provider -->
<SMSPassword>[illegible]</SMSPassword>    <!-- User password of the sms provider -->
<SMSOriginator>Kendox AG</SMSOriginator>  <!-- Sender -> Max. 11 characters -->
<SMSText>
  <!-- The placeholder {0} will be replaced with the verificaton code -->
  <de>
    RIA Client - Zwei Faktor Authentifizierung
    Sicherheitscode: {0}
  </de>
  <en>
    RIA Client - Two Factor Authentication
    Security code: {0}
  </en>
</SMSText>
<EmailSubject>
  <de>RIA Client - Zwei Faktor Authentifizierung</de>
  <en>RIA Client - Two Factor Authentication</en>
</EmailSubject>
<EmailText>
  <!-- The placeholder {0} will be replaced with the verificaton code -->
  <de>Sicherheitscode: {0}</de>
  <en>Security code: {0}</en>
</EmailText>
<IsCaseSensitive>false</IsCaseSensitive>    <!-- If true, the verification code validation is case sensitive -->
<VerificationCodeMask>#####</VerificationCodeMask>
<!--
    Is used to generate the verification code for the Two Factor Authentication by mask. The mask can contain the following special characters:

     # : a digit ->                                  "1234567890"
     a : an alphabetic caracter (upper and lower case) ->    "abcdefghijkmnopqrstuvwxyzABCDEFGHKLMNPQRSTUVWXYZ"
     A : an alphabetic character (upper case) ->             "ABCDEFGHKLMNPQRSTUVWXYZ"
     n : an alphanumeric character (upper and lower case) -> "abcdefghijkmnopqrstuvwxyzABCDEFGHKLMNPQRSTUVWXYZ123456789"
     N : an alphanumeric character (upper case) ->           "ABCDEFGHKLMNPQRSTUVWXYZ123456789"


    All other characters are taken literally. If not specified, the Mask is "######" by default.

    Usage:
    <VerificationCodeMask>NNNN</VerificationCodeMask>
  -->
```

Code-Definitionen

Aktivierung/Deaktivierung der Funktion

<TwoFactorAuthentication>false</TwoFactorAuthentication>

In folgenden Abschnitt innerhalb des XML's wird die SMS-Fähigkeit konfiguriert

Provider mit Login

<SMSProvider>aspsms.com</SMSProvider> (→als Beispiel bei Verwendung in CH)
<SMSUserKey></SMSUserKey>
<SMSPassword></SMSPassword>
<SMSOriginator>Kendox AG</SMSOriginator>

Definition des SMS Inhalts

```
<SMSText>
   <de>
    RIA Client - Zwei Faktor Authentifizierung
    Sicherheitscode: {0}
   </de>
   <en>
    RIA Client - Two Factor Authentication
    Security code: {0}
   </en>
</SMSText>
```

Definition des E-Mail Inhalts

```
<EmailSubject>
  <de>RIA Client - Zwei Faktor Authentifizierung</de>
  <en>RIA Client - Two Factor Authentication</en>
</EmailSubject>
<EmailText>
   <de>Sicherheitscode: {0}</de>
   <en>Security code: {0}</en>
</EmailText>
```

Groß/Kleinschreibung

```
<IsCaseSensitive>false</IsCaseSensitive>
```

Authentifizierungscode Definition

```
<VerificationCodeMask>#####</VerificationCodeMask>
```

- ➔ Im Tag <VerificationCodeMask> wird beim default Wert „######“ ein sechsstelliger Zahlencode ermittelt.
- ➔ Die Komplexität des Codes kann jedoch nach folgenden Kriterium gewählt werden:

: eine Zahl:
"1234567890"
a : alphanumerische Kombination (Groß und Kleinschreibung):
"abcdefghijkmnopqrstuvwxyzABCDEFGHKLMNPQRSTUVWXYZ"
A : Buchstaben Kombination (Großschreibung):
"ABCDEFGHKLMNPQRSTUVWXYZ"
n : alphanumerische Kombination (Groß und Kleinschreibung):
"abcdefghijkmnopqrstuvwxyzABCDEFGHKLMNPQRSTUVWXYZ123456789"
N : alphanumerische Kombination (Großschreibung):
"ABCDEFGHKLMNPQRSTUVWXYZ123456789"

13 Formularauthentifizierung (keine ADS-Integration)

Die in diesem Kapitel beschriebenen Einstellungen müssen vorgenommen werden, wenn Kendox WebService mit „Formularauthentifizierung“ betrieben werden soll.

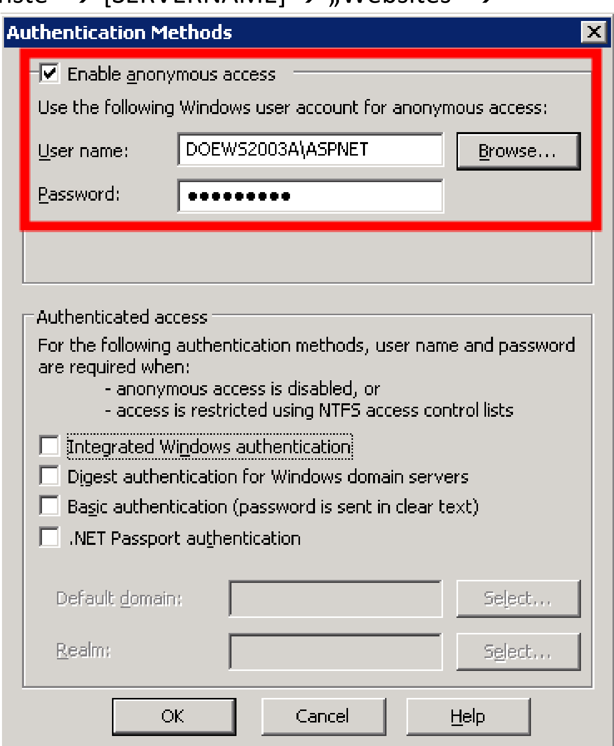


Hinweis: Aus den Überschriften der folgenden Unterkapitel kann die IIS-Version entnommen werden, für die das Unterkapitel gültig ist. Soll z. B. ein IIS 6.x konfiguriert werden, müssen alle Anweisungen in den Unterkapiteln ausgeführt werden, die in der Überschrift „IIS 6.x“ beinhalten.

13.1 Authentifizierungsmethoden unter IIS 5.x/6.x

Im IIS 5.x/6.x müssen der „Anonyme Zugriff“ aktiviert und die „Integrierte Windows-Authentifizierung“ deaktiviert werden. Die Einstellungen sind im Fenster „Authentifizierungsmethoden“ zu finden.

Das Fenster „Authentifizierungsmethoden“ kann über „Start“ → „Alle Programme“ → „Verwaltung“ → „Internet-Informationsdienste“ → [SERVERNAME] → „Websites“ → „Standardwebsite“ → Rechtsklick auf „KXWebService“ → „Eigenschaften“ → „Verzeichnissicherheit“ → „Steuerung des anonymen Zugriffs und der Authentifizierung“ erreicht werden.



Für den anonymen Zugriff kann der Benutzer „ASPNET“ ausgewählt werden. Bevorzugt wird auch der Benutzer „Netzwerkdienst“ verwendet, da dieser für eigens für Webdienste gedacht ist. Dies bewirkt, dass für die Anmeldung am WebServer der Benutzer „ASPNET“ verwendet wird. Nach erfolgter Anmeldung läuft der IIS-Prozess unter dem Benutzer „ASPNET“.

Für alle Verzeichnisberechtigungen muss der Benutzer „ASPNET“ verwendet werden. Nähere Informationen dazu können im Kapitel „Verzeichnisberechtigungen (IIS 5.x/6.x/7.x) nachgeschlagen werden.

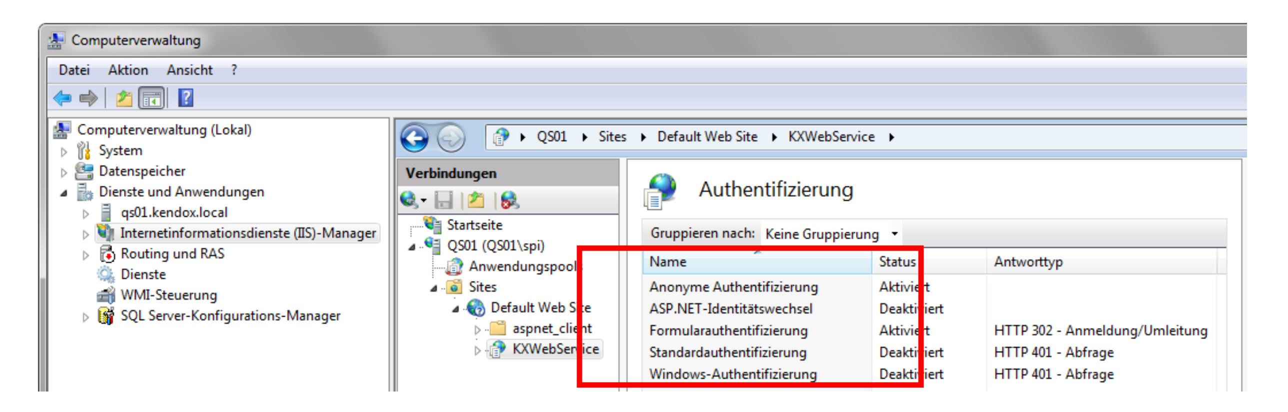
Darüber hinaus müssen in der Datei Web.config folgende Tags manuell verändert werden, da die Konfiguration im UI nicht in die Datei Web.config übernommen werden:

```
<authentication mode="Forms"/>
<identity impersonate="false"/>
```

Siehe Kapitel Web.Config (IIS 5.x/6.x/7.x)

13.2 Authentifizierungsmethoden unter IIS 7.x

Im IIS 7.x müssen „Anonyme Authentifizierung“ und „Formularauthentifizierung“ aktiviert und alle anderen Punkte deaktiviert werden. Diese sind im Fenster „Authentifizierung“ zu finden.



Im neu geöffneten Bereich müssen nun die folgenden Authentifizierungen aktiviert / deaktiviert sein (resp. werden):

- Anonyme Authentifizierung:	Aktiviert
- ASP.NET-Identitätswechsel:	Deaktiviert
- Formularauthentifizierung:	Aktiviert
- Standardauthentifizierung:	Deaktiviert
- Windows-Authentifizierung:	Deaktiviert

13.3 Verzeichnisberechtigungen für Network Service (IIS 5.x/6.x/7.x)

Es muss sichergestellt werden, dass folgende Verzeichnisse die beschriebenen Berechtigungen besitzen.

→Der Benutzer „Network Service“ ist derjenige Benutzer, dem der Application Pool (und somit WebService) läuft.



Hinweis: In folgender Tabelle werden alle Berechtigungen für den Benutzer „Netzwerkdienst“ gesetzt. Dies ist unter der Annahme, dass der Kendox WebService unter diesem Benutzer läuft. Wird ein anderer Benutzer für den WebService verwendet, müssen alle Berechtigungen für diesen Benutzer gesetzt werden. Der Benutzer „Netzwerkdienst“ wird als Platzhalter für den tatsächlichen Benutzer verwendet.

Berechtigung: Vollzugriff für den Benutzer „Netzwerkdienst"	
Verzeichnis	Beschreibung
C:\WINDOWS\Microsoft.NET\Framework\ v4.0.30319\Temporary ASP.NET Files\	Da Kendox WebService beim ersten Start kompiliert wird, muss der Benutzer Netzwerkdienst auf das Microsoft.NET-Framework (temporäres Verzeichnis vom .NET Framework) Vollzugriff haben.
Das Tag „<TempDirectory>" befindet sich in der Datei „ConnectionPoolSettings.xml".	Der Benutzer „Netzwerkdienst" muss auf das angegebene Verzeichnis im Tag „<TempDirectory>" Vollzugriff besitzen (siehe Kapitel „Code-Definitionen" für die Tagbeschreibungen).
Berechtigung: Lese- und Schreib- und Ausführungsberechtigung für den Benutzer „Netzwerkdienst"	
Verzeichnis	Beschreibung
Rootverzeichnis (inkl. Unterverzeichnisse!), in welchem Kendox WebService installiert ist. Standardmässig: „C:\Inetpub\wwwroot\KxWebService\".	Der Benutzer „Netzwerkdienst" muss Lese- und Ausführungszugriff auf das Rootverzeichnis und dessen Unterverzeichnisse haben, in dem Kendox WebService installiert ist. Die Lese- und Ausführungsberechtigung muss zwingend vererbt werden.
Berechtigung: Lese- und Schreibberechtigung den Benutzer „Netzwerkdienst"	
Verzeichnis	Beschreibung
C:\WINDOWS\Temp\	Damit von Kendox WebService Dokumente richtig exportiert werden können, muss der Benutzer „Netzwerkdienst" Zugriff auf das temporäre Verzeichnis von Windows besitzen.
Berechtigung: Lese- und Schreibberechtigung für den Benutzer „Netzwerkdienst"	
Verzeichnis	Beschreibung
[Installationsverzeichnis von Kendox WebService]\ KXWebServiceTemp" (standardmässig unter „C:\Inetpub\wwwroot\KxWebService\KXWebServiceTemp")	Diverse temporäre Dateien (ConnectionPoolCredentials.xml, TokenEncryptionData.key, UpDownloadManagerTransactions.xml und XMLEncryptionData.key) werden ins

	KxWebServiceTemp-Verzeichnis. Hierfür benötigen alle Benutzer Lese- und Schreibzugriffe.

Berechtigung: Leseberechtigung für den Benutzer „Netzwerkdienst“	
Verzeichnis	Beschreibung
[Installationsverzeichnis von Kendox WebService]\Licenses“. Standardmässig: „C:\Inetpub\wwwroot\KxWebService\Licenses\“.	Der Benutzer „Netzwerkdienst“ muss auf das Verzeichnis und den darunterliegenden Verzeichnissen und Dateien Lesezugriff besitzen.

Web.Config (IIS 5.x/6.x/7.x)

Um die Formularauthentifizierung zu aktivieren, müssen in der Datei „Web.Config“ (standardmässig in C:\Inetpub\wwwroot\KxWebService“) die folgenden Einträge gesetzt werden:

```
<identity impersonate="false" />
<authentication mode="Forms">
```

Dies bewirkt, dass der IIS-Worker Prozess unter dem Benutzer Network Service läuft.



Hinweis: Unter IIS 7.x bewirkt die Änderung der Authentifizierung im UI auch die Änderung in der Web.config und umgekehrt. Trotzdem sollte kontrolliert werden, ob beide Stellen (UI und Web.config) richtig konfiguriert sind, falls Probleme auftreten.

---

14 Java Enabling

Der Kendox WebService kann auch aus Java-Anwendungen konsumiert werden. Um die nötigen Klassen für einen Java-Client zu erzeugen gibt es 2 Möglichkeiten:

14.1 Generierung mit Axis 2

Axis 2 ist ein von Apache zur Verfügung gestelltes Framework , welches eine einfache Generierung von Java-Client WebServicce-Stubs ermöglicht. Getestet wurde die Client Generierung mit Axis 2 Version 1.5.6 und höher. Frühere Versionen von Axis2 können Probleme bei der Generierung verursachen. Axis2 kann von der Homepage von Apache gratis heruntergeladen und installiert werden. Für die Erzeugung der Java-Client WebService Stubs-Klassen kann das Kommandozeilentool "**wsdl2java**" verwendet werden. Dieses Tool kann auch über das Eclipse-Plugin Axis Code Generator aufgerufen werden. Das Plugin ist ebenfalls bei Apache erhältlich.

14.2 Generierung mit JAX-WS

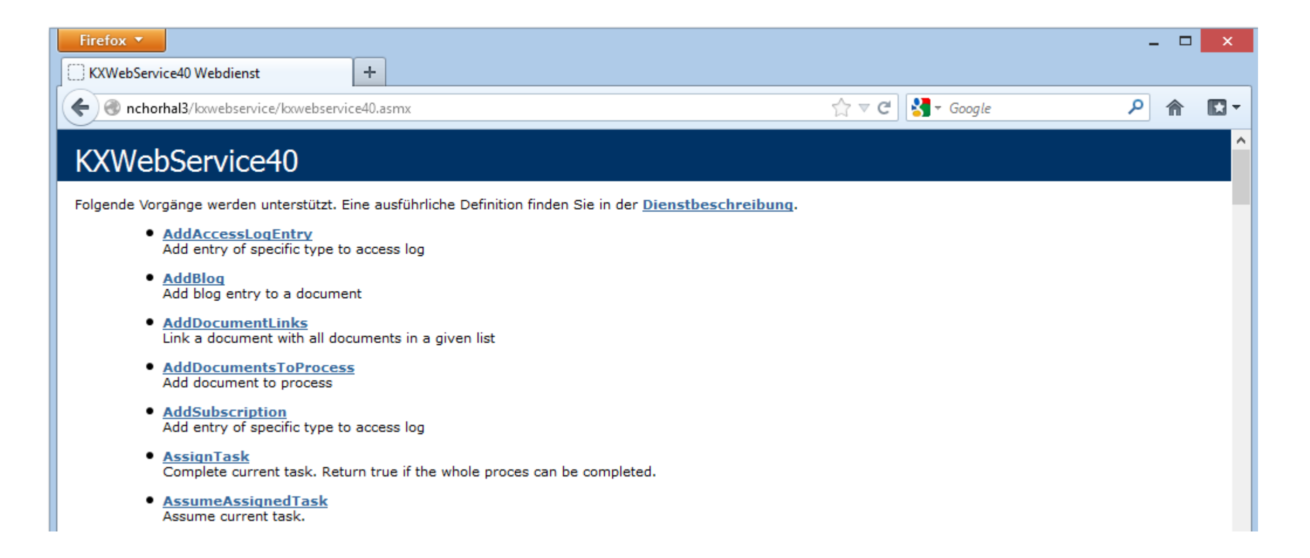
"**JAX-WS**" ist eine API zur Erzeugung und Einbindung von WebServices. JAX-WS ist ab Version 1.5 im JDK enthalten. Für die Client-Generierung mit JAX-WS muss die Web.config-Datei des Kendox WebServices angepasst werden. Die Einträge <add name="HttpPost"/> und <add name="HttpGet"/> müssen auskommentiert werden.

Nach einem erneuten Aufruf des Kendox WebServices im Browser wurde die WSDL-Datei des WebServices neu generiert und kann mit JAX-WS verarbeitet werden. Für die Generierung der Java WebService Stubs-Klassen kann das Kommandozeilentool "**wsimport**" verwendet werden.

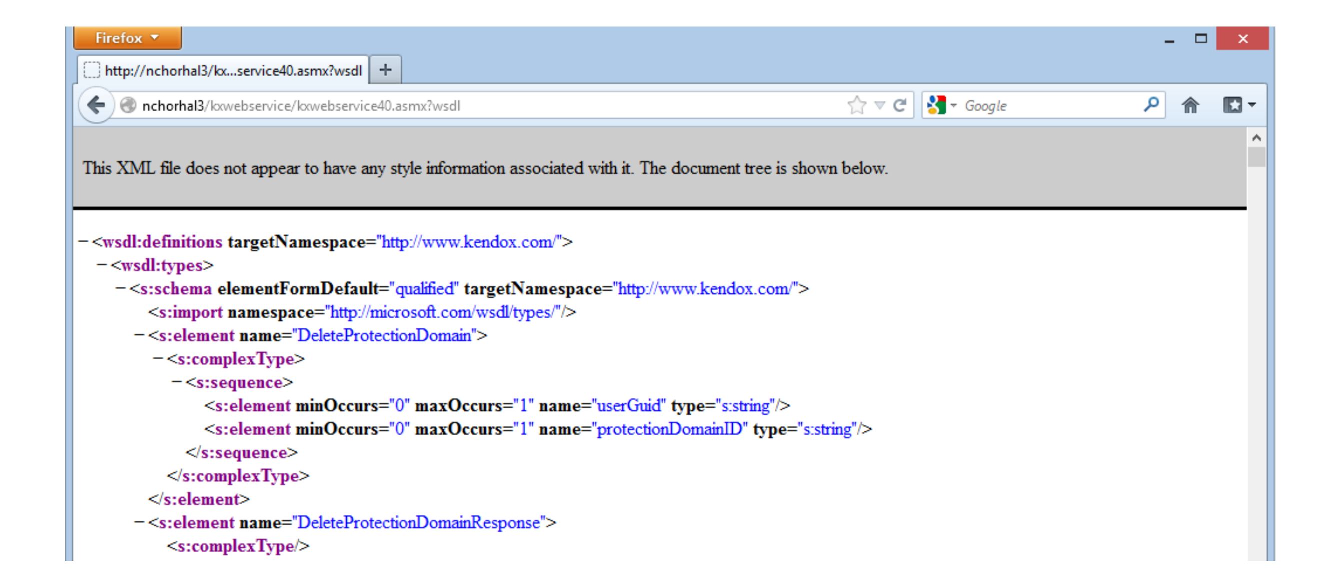
15 Kendox WebService-Bindung

Kendox WebService wird mit folgender URL aufgerufen:
http://[Hostname]/[WebService-Verzeichnisname]/KXWebService40.asmx

(z. B. http://localhost/KXWebService/KXWebService40.asmx)
Diese URL dient für die WebService-Bindung für InfoShare-Integrationen.



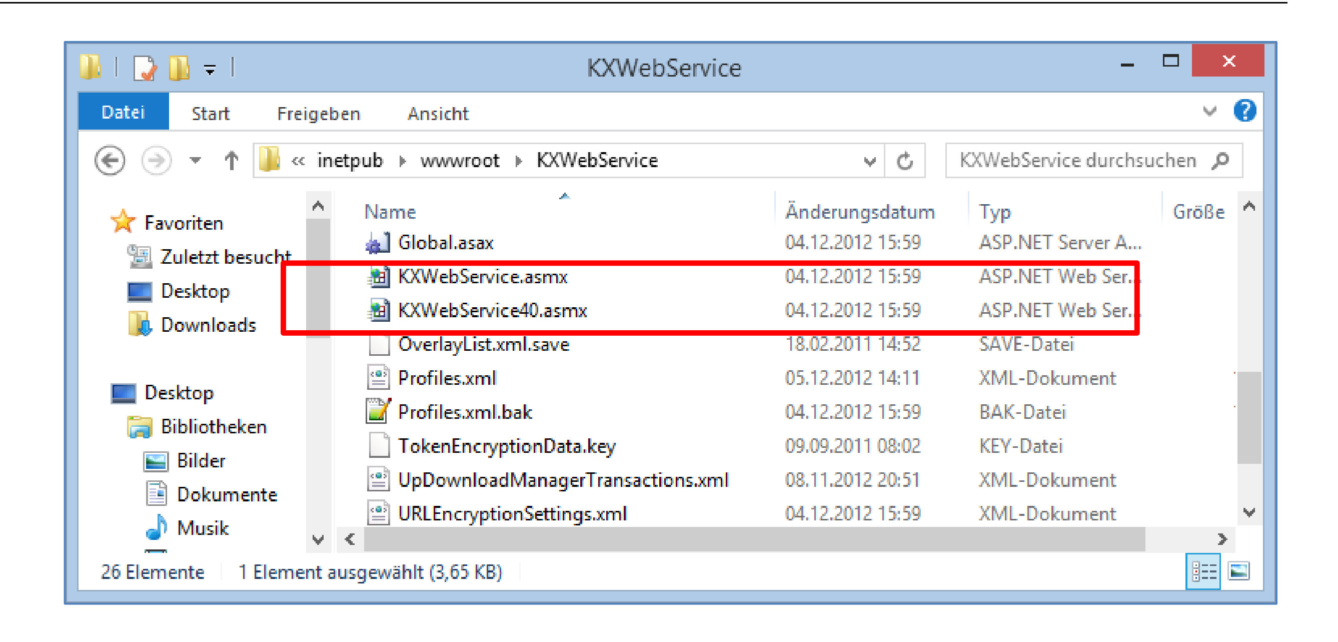
In einigen Fällen (z. B. für Java-basierende Integrationen) wird die WSDL-Datei für die WebService-Bindung benötigt. Die WSDL-Datei erhält man über folgenden Aufruf:
http://[Hostname]/[WebService-Verzeichnisname]/KXWebService40.asmx?WSDL
(z. B. http://localhost/KXWebService/KXWebService40.asmx?WSDL)



Ab Version 4.0 wird die neue WebService Aufrufdatei *„KxWebService40.asmx"* Datei mitausgeliefert, die neue Funktionen zu InfoShare 4.0 beinhaltet. Drittanwendungen die die neuen Funktionen zu InfoShare.Server 4.0 nutzen wollen, müssen auf die neue *„KxWebService40.asmx"* umsteigen.



Achtung: Drittanwendungen die die neuen Funktionen zu InfoShare.Server 4.0 nutzen wollen, müssen auf die neue *„KxWebService40.asmx"* umsteigen. Aus Kompatibilitätsgründen wird die *„KxWebService.asmx"* Datei mit ausgeliefert.

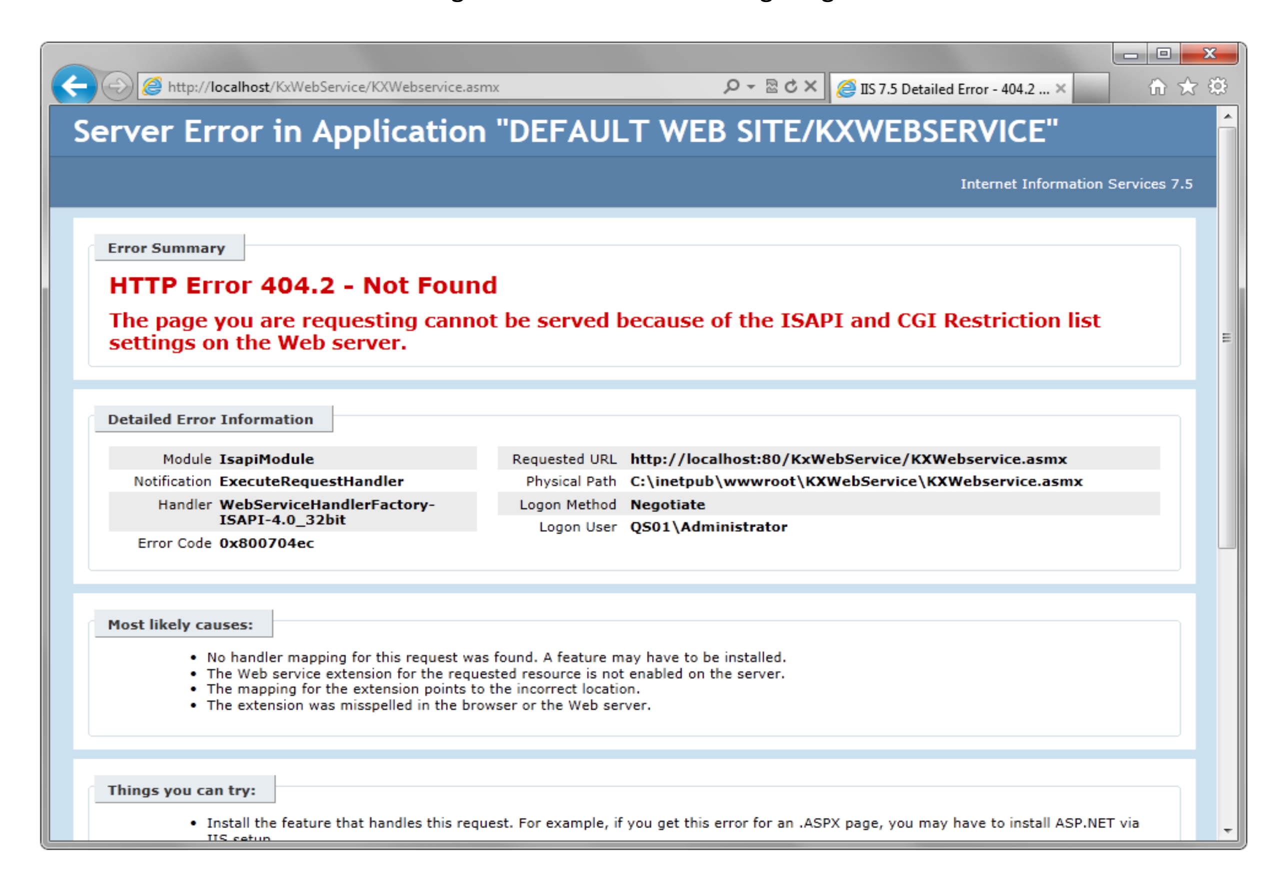


16 Fehlerbehebung

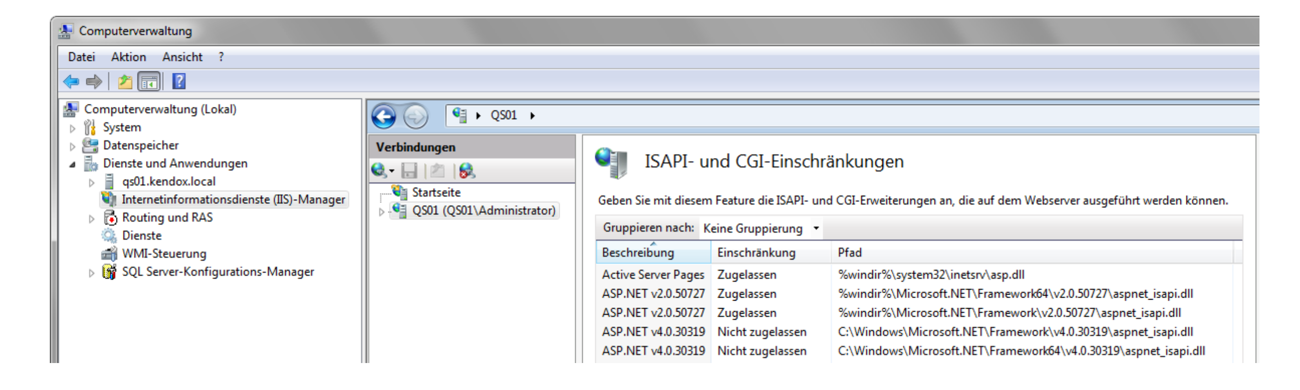
In diesem Abschnitt werden mögliche Fehler und dessen Behebung beschrieben.

16.1 ISAPI / CGI Fehler

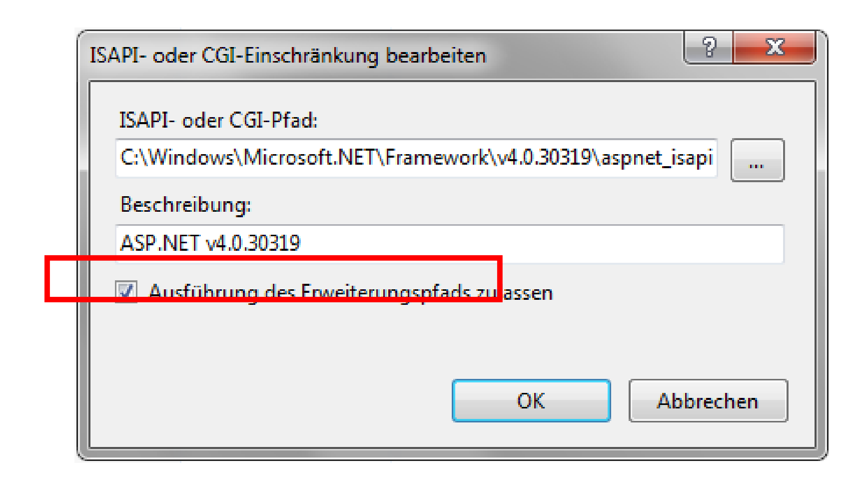
Nach der Installation wird der Zugriff für Framework 4.0 auf ISAPI / CGI standardmässig blockiert. Beim Aufrufen von Kendox WebService („KXWEbService.asmx“) kann ohne Zugriff auf das Framework 4.0 die Fehlermeldung „The page you are requesting cannot be served because of the ISAPI and CGI Restriction list settings on the Web server.“ angezeigt werden:



Um dieses Problem zu beheben, muss die Einschränkung von ISAPI- und CGI-Einschränkungen für ASP.NET Framework 4.0 aufgehoben werden. Unter „Computerverwaltung“ → „Dienste und Anwendungen → „Internetinformationsdienste (IIS)-Manager“ →“[SERVERNAME]\Administrator“ → „ISAPI- und CGI-Einschränkungen“ muss die Einschränkung für ASP.NET v4.0 aufgehoben werden:



Mit einem Doppelklick auf die entsprechende Version erscheint ein Fenster, in welchem die Ausführung des Erweiterungspfads zugelassen werden muss:

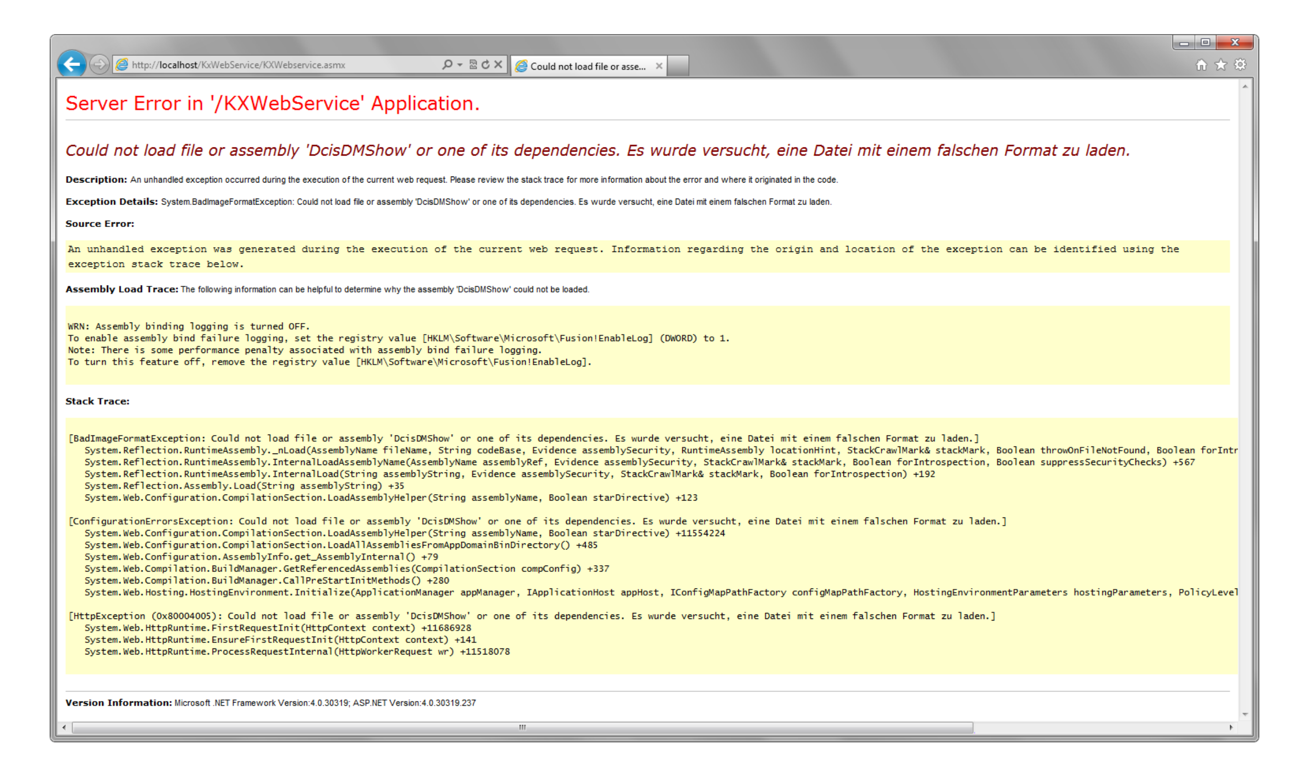


Nun sollte die Seite (z. B. http://localhost/KxWebService/KXWebservice.asmx) aufrufbar sein.

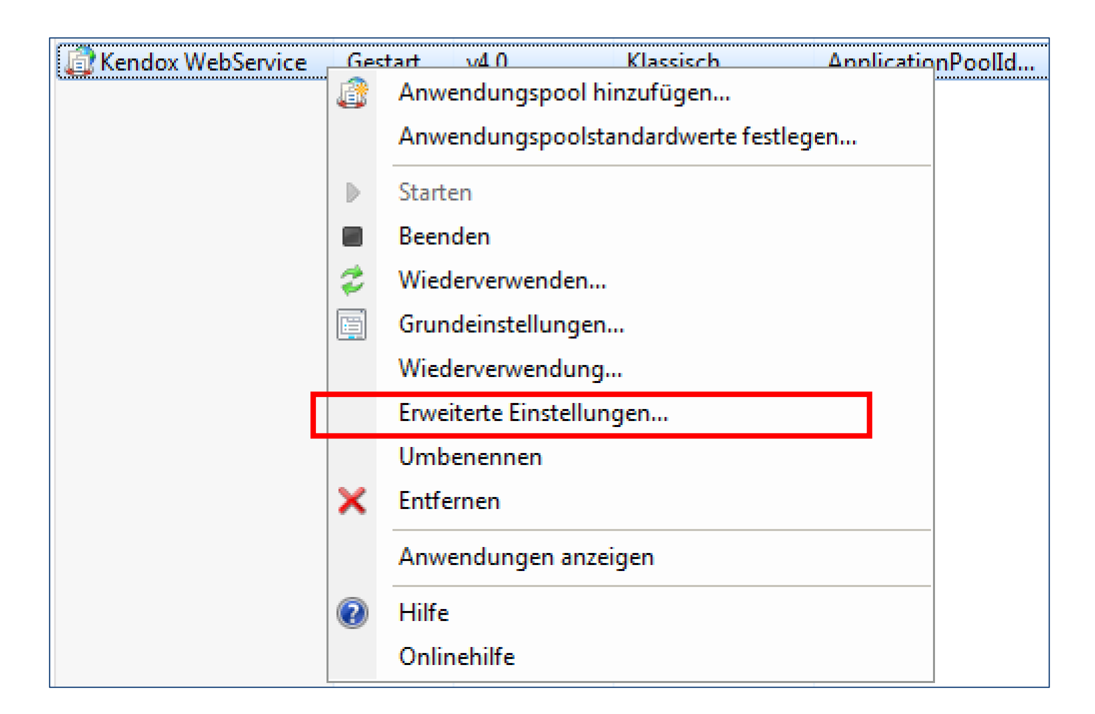
16.2 DcisDMShow Fehler

Beim Öffnen von http://localhost/KxWebService/KXWebservice.asmx kann folgende Fehlermeldung erscheinen:

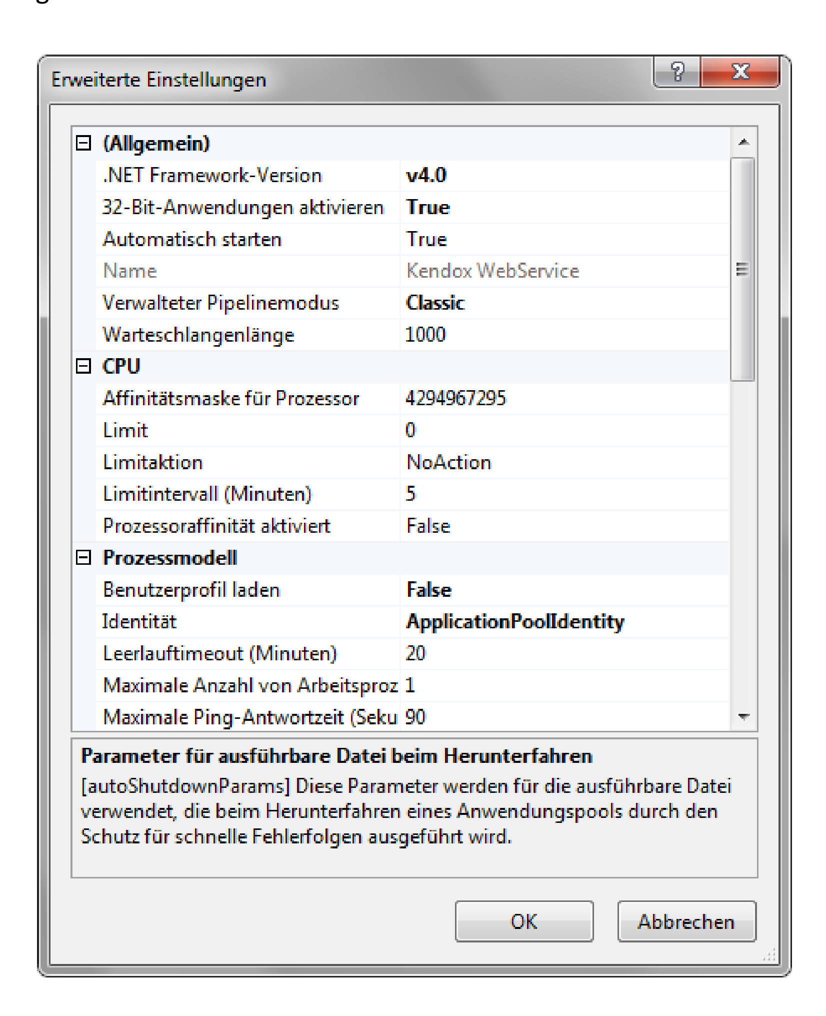
Error in '/KXWebService' Application.
Could not load file or assembly 'DcisDMShow' or one of its dependencies. Es wurde versucht, eine Datei mit einem falschen Format zu laden.



Um dieses Problem zu beheben, muss der für Kendox WebService verwendete Anwendungspool konfiguriert werden. Im Server-Manager unter „Rollen“ → Webserver (IIS) → Internetinformationsdienste (IIS)-Manager → [SERVERNAME] → Anwendungspools muss hierzu der entsprechende Anwendungspool ausgewählt und mittels Rechtsklick darauf die „erweiterten Einstellungen…“ geöffnet werden:



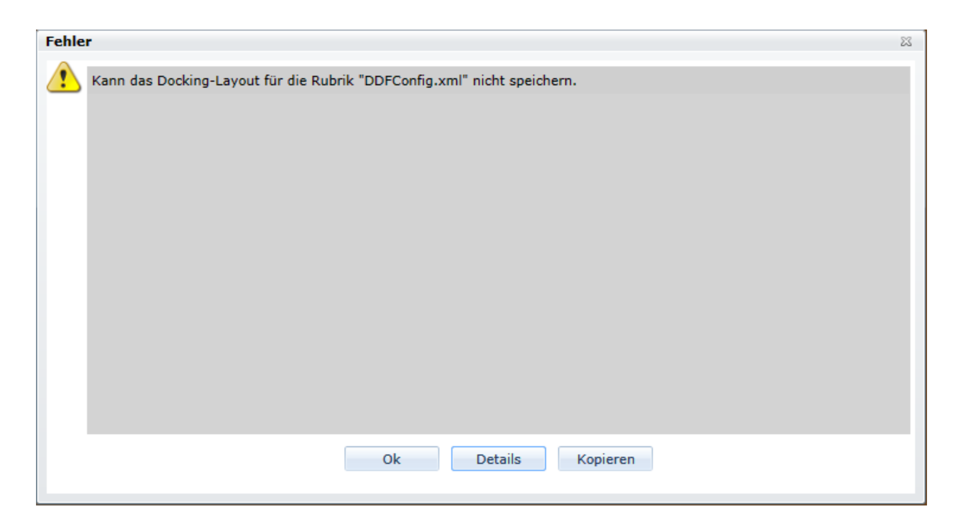
Im neu geöffneten Fenster muss „32-Bit-Anwendungen aktivieren“ von „False“ auf „True“ geändert werden:



Nun sollte die Seite (z. B. http://localhost/KxWebService/KXWebservice.asmx) aufrufbar sein.

16.3 Docking-Layout aus RIA.Client kann nicht gespeichert werden

Sollte aus dem Kendox RIA.Client die Docking-Layouts eines Benutzers nicht gespeichert werden können, wird folgende Fehlermeldung angezeigt.



Dies ist darauf zurückzuführen, dass im „<TempDirectory>“-Verzeichnis, welches in der Datei „ConnectionPoolSettings.xml“ definiert ist, der Benutzer, der den Kendox WebService ausführt, KEINE Schreibrechte auf die Dateien und darin enthaltenen Verzeichnisse hat. Damit die Layouts gespeichert werden können, muss die Schreibberechtigung auf folgende Verzeichnisse gesetzt werden:

- DockingLayouts
- DockingLayouts\Templates
- AnnotationTemplates

17 Systemvoraussetzungen

Die Systemvoraussetzungen definieren die **Mindestanforderungen**, die erfüllt werden müssen, damit die Anwendung ordnungsgemäss funktioniert.

Kendox testet laufend die folgenden Einstellungen. Alle anderen Konfigurationen wurden nicht oder nur teilweise getestet!

Hardware	
	Intel Pentium 3 (1GHz)
	512MB RAM
	250MB freier Festplattenspeicher
Software	
	Microsoft Windows Server 2003 oder höher
	Microsoft .NET Framework 4.0
	IIS 6 oder höher (32-Bit-Modus)



Kendox AG
Hauptsitz
Bahnhof-Strasse 7
9463 Oberriet SG
Schweiz

T +41 (71) 763 72 72
F +41 (71) 763 72 71

Kendox AG
Niederlassung Österreich
Lassallestraße 7b
1020 Wien
Österreich

T +43 (1) 212 78 97

Kendox AG
Niederlassung Deutschland
Industriestraße 25
91710 Gunzenhausen
Deutschland

T +49 (9831) 505 – 335

www.kendox.com | info@kendox.com
